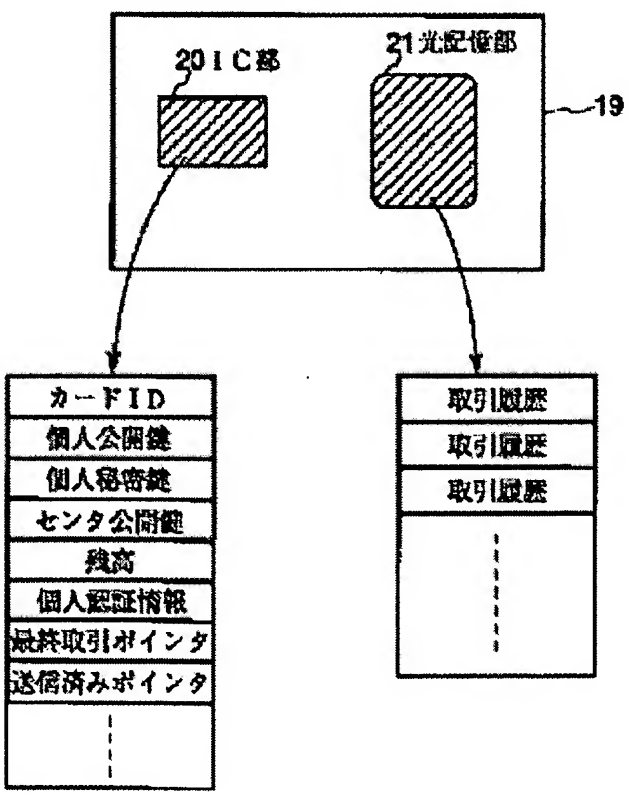
ELECTRONIC MONEY SYSTEM AND RECORDING MEDIUM

Publication number: JP10154192
Publication date: 1998-06-09
Inventor: FURUHASHI NOBUO; HETA SATOSHI; SHIBATA ATSUSHI; SATO SATORU
Applicant: NTT DATA TSUSHIN KK
Classification:
- international: ***G07D9/00; G06F19/00; G06K17/00; G06Q10/00; G06Q20/00; G06Q40/00; G06Q50/00; G07F7/08; G07F19/00;*** **G07D9/00; G06F19/00; G06K17/00; G06Q10/00; G06Q20/00; G06Q40/00; G06Q50/00; G07F7/08; G07F19/00;** (IPC1-7): G06F19/00; G06K17/00; G07D9/00; G07F7/08; G07F19/00
- European:
Application number: JP19970251907 19970917
Priority number(s): JP19970251907 19970917; JP19960255947 19960927

Abstract of **JP10154192**

PROBLEM TO BE SOLVED: To effectively prevent the forgery, etc., of money data and also to easily detect an illegal transaction. SOLUTION: In an electronic money system in which electronic money is transacted by using an electronic money card 19 that stores electronic money having a money value, what is provided with an IC part 20 and an optical storing part 21 is used as the card 19. The part 20 records information which specifies the card 19, the balance, information that accesses the part 21, etc., and the part 21 records the entire history of electronic money transactions which are performed by using the electronic money card. The transaction history is also registered in a computer of an electronic money transaction system. The occurrence place of illegality, the amount of a sum, etc., are detected by tracking the transaction history.



Japanese Publication number : 10-154192 A

CLAIMS

[Claim(s)]

[Claim 1]A computer connected with an electronic money card which is provided with an added type storage parts store of a postscript and an IC memory part characterized by comprising the following, and stores information about a monetary value, two or more terminals which process this electronic money card, and a terminal of this plurality by a communication line, and an electronic money system constituted more.

An input means which inputs directions and transaction money amount of said added type storage parts store of a postscript memorizing transaction history information, said IC memory part memorizing position information which shows the final position of transaction history information memorized by said added type storage parts store of a postscript, and said two or more terminals storing information about a monetary value in said electronic money card.

A directions wording-of-a-telegram transmitting means which transmits to said computer by making into a charge request message account specific information for specifying directions and transaction money amount which were inputted by said input means, and an account.

A means by which a preparation and said computer receive said charge request message.

An amount-of-money transportation device which moves the amount of money which transaction money amount shows from an account which account specific information in said charge request message which received specifies to a predetermined account, Have a reply telegraphic message transmitting means which transmits a reply telegraphic message which shows that movement of the amount of money by said amount-of-money transportation device was completed, and said two or more terminals, A means which writes transaction history information corresponding to said reply telegraphic message in said added type storage parts store of a postscript according to position information which answered reception of said reply telegraphic message and was stored in said IC memory part.

[Claim 2]The electronic money system according to claim 1 characterized by what a pit is formed physically, data is written in and said added type storage parts store of said electronic money card of a postscript comprises an optical storing part which is not rewritable for by irradiating light energy.

[Claim 3]At least one side of said added type storage parts store of said electronic money card of a postscript and said IC memory part, The electronic money system according to claim 1 or 2 which has memorized said account specific information and is characterized by what said directions wording-of-a-telegram transmitting means is constituted more for with a means which reads said account specific information memorized by said electronic money card, and a means to transmit read account specific information.
[Claim 4]If said computer distinguishes whether it is more than the transaction money amount in which the balance of an account specified by said account specific information is directed by said charge request message and the balance becomes in this less than transaction money amount, The electronic money system according to claim 1, 2, or 3 characterized by what it has a means to transmit an error message to said terminal, and to stop dealings for.
[Claim 5]An electronic money system given in any 1 paragraph of claims 1 thru/or 4 characterized by what it is [a thing] characterized by comprising the following.
Said transaction history information is the classification of dealings about each dealings.
A dealings date.
Information which specifies said terminal which processed the dealings.
Transaction money amount.

[Claim 6]An electronic money system given in any 1 paragraph of claims 1 thru/or 5 characterized by what said added type storage parts store of said electronic money card of a postscript memorizes a transaction history of all the dealings dealt with with this electronic money card for.
[Claim 7]An electronic money system given in any 1 paragraph of claims 1 thru/or 6 characterized by what said computer is provided with a transaction history memory measure which memorizes a transaction history of all the dealings of electronic money of said electronic money card for.
[Claim 8]At least one side of said added type storage parts store of said electronic money card of a postscript and said IC memory part memorizes card identity numerals of the electronic money card, Said charge request message including said card identity numerals said computer, A wrong card ID storage means which memorizes said card identity numerals of said electronic money card which does not accept use as wrong card ID, If said wrong card ID memorized by said card identity numerals contained in said charge request message and said wrong card ID storage means is compared and wrong card ID in agreement is detected, An electronic money system given in any 1 paragraph of claims 1 thru/or 7 characterized by what it has a means to stop dealings for.
[Claim 9]Each aforementioned terminal memorizes terminal identification numerals, and said charge request message including said terminal identification numerals said computer, An unjust terminal ID storage means which memorizes said terminal identification numerals of said terminal which does not accept use as unjust terminal ID, An electronic money system given in any 1 paragraph of claims 1 thru/or 8 characterized

by what it will have a means to stop dealings for if unjust terminal ID in agreement is detected as compared with said unjust terminal ID memorized by said unjust terminal ID storage means in said terminal identification numerals contained in said charge request message.

[Claim 10]It has further a certificate authority provided with an individual information storage means which said IC memory part memorizes an individual public key and an individual secret key of a couple, and memorizes two or more said individual public keys of said electronic money card, Said charge request message including said individual public key of said electronic money card said computer, Have a personal key transmitting means which transmits said individual public key to said certificate authority among charge request messages which received, and said certificate authority, It is distinguished whether it is in agreement with either of two or more individual public keys memorized by said individual information storage means in said received individual public key, An electronic money system given in any 1 paragraph of claims 1 thru/or 9 characterized by what it has further a means to stop dealings by transmitting a message of a purport [that it cannot trade] to said terminal for when not in agreement.

[Claim 11]Said added type storage parts store of a postscript or said IC memory part memorizes card identity numerals, Have further a certificate authority provided with an individual information storage means which memorizes two or more said card identity numerals of said electronic money card, and said charge request message, Including said card identity numerals, said computer, Have a means to transmit card identity numerals which received to said certificate authority, and said certificate authority, It is distinguished whether it is in agreement with either of two or more card identity numerals memorized by said individual information storage means in said card identity numerals which received, An electronic money system given in any 1 paragraph of claims 1 thru/or 9 characterized by what it has further a means to transmit a message of a purport [that it cannot trade] to said terminal, and to stop dealings for when not in agreement.

[Claim 12]Each aforementioned IC memory part is provided with an individual public key and an individual secret key of a couple, and each aforementioned terminal, Have a terminal public key and a terminal secret key of a couple, and said charge request message, Information about dealings, and the 1st attestation child generated with said electronic money card using said individual secret key, Including information about said dealings, the 2nd attestation child generated with said terminal using said terminal secret key, said individual public key, and said terminal public key, said computer, An electronic money system given in any 1 paragraph of claims 1 thru/or 11 which distinguish whether the said 1st and 2nd attestation child is in agreement using said individual public key and said terminal public key, and are characterized by what processing for performing said charge is performed for only when in agreement.

[Claim 13]An electronic money system given in any 1 paragraph of claims 1 thru/or 12 characterized by what a transaction history memorized by added type storage parts store of said electronic money card of a postscript does not include information which specifies

this electronic money card for.
[Claim 14]An electronic money system given in any 1 paragraph of claims 1 thru/or 13 characterized by what it is [a thing] characterized by comprising the following.
An acquisition means from which one side of said IC memory part of said electronic money card and said added type storage parts store of a postscript has memorized characteristic data in which a user's bodily features is shown, and said two or more terminals acquire characteristic data in which an operator's bodily features is shown.
A reading means which reads characteristic data from said electronic money card.
A discriminating means which distinguishes whether characteristic data acquired by said acquisition means is compared with characteristic data read by said reading means, and it. is substantially in agreement.
A dealings control means which forbids dealings of electronic money through this terminal when it judges that dealings of electronic money through this terminal are enabled, and said discriminating means is not substantially in agreement when it judges that said discriminating means is substantially in agreement.

[Claim 15]An electronic money system characterized by comprising the following for trading in electronic money which is the electronic information which has a monetary value.
The 1st memory measure that memorizes card identity numerals for specifying information and self about said electronic money which contains the balance at least.
The 2nd memory measure that memorizes a transaction history of said electronic money.
Two or more electronic money cards which it has.
A bank center provided with a settlement account corresponding to each aforementioned electronic money card, Terminal identification numerals for specifying self are attached, and it is equipped with said electronic money card, A charge request input means for inputting a charge demand it is directed that supplements an electronic money card equipped with said electronic money of prescribed amount of money, and a charge demand transmitting means which transmits said charge demand.

[Claim 16]The electronic money system according to claim 15 characterized by what it is [a thing] characterized by comprising the following.
A means to transmit an error message to said electronic money transaction device if said computer distinguishes whether it is said more than prescribed amount of money in which the balance of said settlement account corresponding to this electronic money card is directed by said charge demand and this balance becomes in this less than prescribed amount of money.
A means to stop dealings.

[Claim 17]The electronic money system according to claim 15 or 16 characterized by what said 1st memory measure is constituted by IC chip provided with a memory in said

electronic money card, and said 2nd memory measure is constituted for by storage which is not rewritable.

[Claim 18]The electronic money system according to claim 15, 16, or 17 characterized by what said transaction history contains said card identity numerals of said electronic money card, and said terminal identification numerals of said electronic money transaction device for.

[Claim 19]The electronic money system according to claim 15, 16, 17, or 18 characterized by what a transaction history recorded on said electronic money card does not include information for specifying the electronic money card itself [this] for.

[Claim 20]The electronic money system according to claim 15, 16, or 17 characterized by what it is [a thing] characterized by comprising the following.

Said transaction history is a dealings date.

Said terminal identification numerals of said electronic money transaction device which transmitted said charge demand.

Transaction money amount.

[Claim 21]An electronic money system given in any 1 paragraph of claims 15 thru/or 20 characterized by what said 2nd memory measure of said electronic money card memorizes a transaction history of all the dealings dealt with with this electronic money card for.

[Claim 22]An electronic money system given in any 1 paragraph of claims 15 thru/or 21 characterized by what said transaction history memory measure of said computer memorizes a transaction history of all the dealings dealt with with said electronic money card for.

[Claim 23]An electronic money system given in any 1 paragraph of claims 15 thru/or 22 an especially more inaccurate electronic money card characterized by comprising the following being detectable.

A charge demand transmitted by said charge demand transmitting means of said electronic money transaction device, A wrong card ID storage means which memorizes said card identity numerals of said electronic money card in which said computer does not accept use as wrong card ID including said card identity numerals of an electronic money card inserted in this electronic money transaction device.

A means to distinguish whether it is in agreement as compared with said wrong card ID memorized by said wrong card ID storage means in said card identity numerals contained in said charge demand.

[Claim 24]An electronic money system given in any 1 paragraph of claims 15 thru/or 23 an especially more inaccurate electronic money transaction device characterized by comprising the following being detectable.

An unjust terminal ID storage means a charge demand transmitted by said charge demand transmitting means of said electronic money transaction device remembers said terminal identification numerals of said electronic money transaction device with which

said computer does not accept use including said terminal identification numerals of this electronic money transaction device to be as unjust terminal ID.
A means to distinguish whether it is in agreement as compared with said unjust terminal ID memorized by said unjust terminal ID storage means in said terminal identification numerals contained in said charge demand.

[Claim 25]Have further a certificate authority which memorizes a registration list of an electronic money card registered into this electronic money system, and said charge demand, Said electronic money card including specific data for specifying said certificate authority, An electronic money system given in any 1 paragraph of claims 15 thru/or 24 characterized by what it has a means to stop dealings for when specific data contained in said charge demand distinguishes whether it registers with a registration list and is not registered in it.
[Claim 26]Said electronic money card is provided with an individual public key and an individual secret key of a couple, and said electronic money transaction device, Have a terminal public key and a terminal secret key of a couple, and said charge demand, Information about dealings, and the 1st attestation child generated using said individual secret key, Including information about said dealings, the 2nd attestation child generated using said terminal secret key, said individual public key, and said terminal public key, said computer, An electronic money system given in any 1 paragraph of claims 15 thru/or 25 characterized by what it is distinguished for whether the said 1st and 2nd attestation child is in agreement using said individual secret key and said terminal secret key.
[Claim 27]An electronic money system given in any 1 paragraph of claims 15 thru/or 26 characterized by what it is [a thing] characterized by comprising the following.
An acquisition means from which one side of said 1st memory measure of said electronic money card and said 2nd memory measure has memorized characteristic data in which a user's bodily features is shown, and said electronic money transaction device acquires characteristic data in which an operator's bodily features is shown.
A reading means which reads characteristic data from said electronic money card.
A discriminating means which distinguishes whether characteristic data acquired by said acquisition means is compared with characteristic data read by said reading means, and it is substantially in agreement.
A dealings control means which forbids dealings of electronic money through this electronic money transaction device when it judges that dealings of electronic money through this electronic money transaction device are enabled, and said discriminating means is not substantially in agreement when it judges that said discriminating means is substantially in agreement.

[Claim 28]An electronic money system which trades in electronic money using an electronic money card which stores electronic money which has a monetary value, comprising:

Said electronic money card is provided with an added type storage parts store of a postscript, and an IC memory part, and said IC memory part, A dealings means to memorize information for accessing information and said added type storage parts store of a postscript for specifying the electronic money card, and to trade in electronic money with which said electronic money system is stored in said electronic money card.
A history recording device which memorizes a history of dealings of electronic money conducted to said added type storage parts store of said electronic money card of a postscript by using this electronic money card.

[Claim 29]The electronic money system according to claim 28 characterized by what said electronic money system is provided with a history storage means which memorizes further a history of dealings of electronic money conducted with this electronic money system for.
[Claim 30]An electronic money system which trades in electronic money using a medium by which electronic money information is recorded, comprising:
A reading means which reads characteristic data about a user's bodily features currently recorded on a medium.
A scanning means which scans the whole or a part of a card user's body.
A means to change into form of data currently recorded through data scanned by said scanning means.
A means to compare data after conversion with data currently recorded on said medium, a means to judge the degree of coincidence by comparison of said data, and a means that validates an electronic money transaction when the above-mentioned decision result is beyond constant value.

[Claim 31]It is the recording medium which recorded a program characterized by comprising the following for making it function as said terminal in a system and in which computer reading is possible, Directions and transaction money amount which were inputted by input means which inputs directions and transaction money amount of storing information concerning a monetary value in this computer in said electronic money card, and said input means, A transmitting means which transmits account specific information for specifying an account to said center as a charge request message, Charge permission wording of a telegram which answered said charge request message and has been returned from said center is received, Position information which shows a position which should write in data is read from said IC memory part of said electronic money card, A recording medium which recorded a program for considering it as a means which writes transaction history information including information about said monetary value in said added type storage parts store of said electronic money card of a postscript according to this position information, and making it function and in which computer reading is possible.
Two or more terminals which process an electronic money card which is provided with an added type storage parts store of a postscript, and an IC memory part for a computer, and

stores information about a monetary value.
A center connected with a terminal of this plurality by communication.

[Claim 32]A computer, As an electronic money transaction device which processes an electronic money card which memorizes electronic money information and card identity numerals in an electronic money system for trading in electronic money which is the electronic information which has a monetary value, and a transaction history of electronic money. Are computer reading good signifier recording media to operate, and this computer, A charge request input means to input a charge demand which requires a supplement to said electronic money card of electronic money of prescribed amount of money, While answering a notice from said center answered and returned to a charge demand transmitting means which transmits said charge demand to a center, and said charge demand and recording a transaction history on said electronic money card, A recording medium which recorded a program for considering it as a card renewal means to add said prescribed amount of money, and making it function on the balance memorized by this electronic money card and in which computer reading is possible.
[Claim 33]A scanning means which scans the whole or a part of a card user's body for a computer, A conversion method which changes into prescribed format data scanned by said scanning means, A reading means which reads characteristic data about a user's bodily features currently recorded on a medium by which electronic money information is recorded, A means to compare data read by said reading means with data changed by said conversion method, A recording medium which recorded a program for considering it as a means which validates an electronic money transaction, and making it function when a means and the above-mentioned decision result which judge the degree of coincidence in comparison of said data are beyond constant value and in which computer reading is possible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the electronic money system which trades in the electronic money which is pocketbook information.
[0002]
[Description of the Prior Art]The electronic money system which enables electronic settlement of accounts using the money data which has money value is indicated by JP,7-111723,B etc.
[0003]
[Problem(s) to be Solved by the Invention]It is necessary to prevent effectively use of those who do not have authority, the copy of money data, forgery, etc. in an electronic money system. When use of the forged money data is discovered, it is desirable that the

distribution channel is pursued and inaccurate origin and forged origin etc. can be discovered. However, the electronic money system which fills such a request is not yet proposed.

[0004]This invention was made in view of the above-mentioned actual condition, and an object of this invention is to provide the electronic money system which can prevent forgery of money data, etc. effectively. This invention detects unjust dealings easily and an object of this invention is to provide the electronic money system excellent in the traceability.

[0005]

[Means for Solving the Problem]In order to attain the above-mentioned purpose, an electronic money system concerning the 1st viewpoint of this invention, An electronic money card which is provided with an added type storage parts store of a postscript, and an IC memory part, and stores information about a monetary value, Are a computer connected with two or more terminals which process this electronic money card, and a terminal of this plurality by a communication line, and an electronic money system constituted more, and said added type storage parts store of a postscript, Memorize transaction history information containing a dealings specific code for specifying dealings, and at least transaction money amount and one side of the balance, and said IC memory part, Memorize position information which shows the final position of transaction history information memorized by said added type storage parts store of a postscript, and said two or more terminals, An input means which inputs directions and transaction money amount of storing information about a monetary value in said electronic money card, A directions wording-of-a-telegram transmitting means which transmits to said computer by making into a charge request message account specific information for specifying directions and transaction money amount which were inputted by said input means, and an account, An amount-of-money transportation device which moves the amount of money which transaction money amount shows from a means by which a preparation and said computer receive said charge request message, and an account which account specific information in said charge request message which received specifies to a predetermined account, Have a reply telegraphic message transmitting means which transmits a reply telegraphic message which shows that movement of the amount of money by said amount-of-money transportation device was completed, and said two or more terminals, Reception of said reply telegraphic message is answered and it has a means which writes transaction history information corresponding to said reply telegraphic message in said added type storage parts store of a postscript according to position information stored in said IC memory part.

[0006]According to such composition, electronic money can be charged to an electronic money card, and various dealings can be conducted to it using charged electronic money. And since a transaction history is recorded on an added type storage parts store of a postscript, when abnormalities occur, a malfeasance etc. can be easily detected by verifying the contents of record of this added type storage parts store of a postscript. The electronic money card should just have a function of an electronic money card as substance, and a box, a disk, a note, a notebook of the shape, etc. are arbitrary. An ordinary savings account, a

checking account, loan account of an account, etc. are arbitrary, and economic grounds which generate electronic money, such as whether it is cash or to be a loan, are arbitrary.

[0007]By irradiating light energy, a pit is formed physically, data is written in and said added type storage parts store of a postscript comprises an optical storing part which is not rewritable, for example.

[0008]At least one side of said added type storage parts store of said electronic money card of a postscript and said IC memory part, Said account specific information is memorized and said directions wording-of-a-telegram transmitting means is constituted more with a means which reads said account specific information memorized by said electronic money card, and a means to transmit read account specific information. As account specific information, the account number itself may be sufficient or an account number and other corresponding numbers, for example, card ID etc., may be sufficient.

[0009]As long as it distinguishes whether it is more than the transaction money amount in which the balance of an account specified by said account specific information is directed by said charge request message and the balance becomes in this less than transaction money amount, said computer transmits an error message to said terminal, and it may be provided with a means to stop dealings. The safety of dealings can be improved by having such composition.

[0010]Said transaction history information is provided with the following.

About each dealings, they are classification of dealings, and a dealings date.

Information which specifies said terminal which processed the dealings.

Transaction money amount.

An unjust part etc. can be distinguished by pursuing these information. In this case, it is desirable to make said added type storage parts store of said electronic money card of a postscript memorize a transaction history of all the dealings dealt with with this electronic money card.

[0011]Said computer may be provided with a transaction history memory measure which memorizes a transaction history of all the dealings dealt with with said electronic money card. By comparing a transaction history registered into an electronic money card, and a transaction history recorded on a computer, injustice etc. can be detected more easily.

[0012]Include card identity numerals for specifying an electronic money card as said charge request message, and to said computer. A wrong card ID storage means which memorizes said card identity numerals of said electronic money card which does not accept use as wrong card ID, If said wrong card ID memorized by said card identity numerals contained in said charge request message and said wrong card ID storage means is compared and wrong card ID in agreement is detected, a means to stop dealings may be arranged. When an invalid card etc. which were registered are used according to such composition, it is detected and dealings can be stopped.

[0013]An unjust terminal ID storage means which memorizes said terminal identification numerals of said terminal which includes said terminal identification numerals in said charge request message, and does not observe use in said computer as unjust terminal ID,

If unjust terminal ID in agreement is detected as compared with said unjust terminal ID memorized by said unjust terminal ID storage means in said terminal identification numerals contained in said charge request message, a means to stop dealings may be arranged. When an accident terminal etc. which were registered are used according to such composition, it is detected and dealings can be stopped.

[0014]An individual public key and/or card identity numerals which were given to each electronic money card may be given, and a certificate authority which distinguishes whether these individual public key and/or card identity numerals are registered into a system may be arranged.

[0015]Each IC memory part is provided with an individual public key and an individual secret key of a couple, and each aforementioned terminal, Have a terminal public key and a terminal secret key of a couple, and said charge request message, Information about dealings, and the 1st attestation child generated with said electronic money card using said individual secret key, Including information about said dealings, the 2nd attestation child generated with said terminal using said terminal secret key, said individual public key, and said terminal public key, said computer, it distinguishes whether the said 1st and 2nd attestation child is in agreement using said individual public key and said terminal public key, and only when in agreement, processing for performing said charge is performed -- it may constitute like. According to such composition, an unauthorized use of an electronic money card can be detected more correctly.

[0016]It may be made for the transaction history memorized by added type storage parts store of said electronic money card of a postscript not to include information which specifies this electronic money card. According to such composition, capacity of an added type storage parts store of a postscript can be used effectively.

[0017]An operator may judge whether it has the authority to use this electronic money system based on an operator's bodily features.

[0018]An electronic money system concerning the 2nd viewpoint of this invention, The 1st memory measure that memorizes card identity numerals for specifying information and self about said electronic money which is an electronic money system for trading in electronic money which is the electronic information which has a monetary value, and contains the balance at least, Two or more electronic money cards provided with the 2nd memory measure that memorizes a transaction history of said electronic money, A bank center provided with a settlement account corresponding to each aforementioned electronic money card, A charge request input means for inputting a charge demand it is directed that terminal identification numerals for specifying self are attached, and it is equipped with said electronic money card, and supplements self with said electronic money of prescribed amount of money, An electronic money transaction device provided with a charge demand transmitting means which transmits said charge demand, According to a balance memory measure which memorizes the balance of two or more of said electronic money cards, and said charge demand from said electronic money transaction device, A charge directing means it is directed to said bank center that moves said prescribed

amount of money to other predetermined accounts from said settlement account corresponding to this electronic money card, and a means to add said prescribed amount of money to the balance of this electronic money card memorized by said balance memory measure, A transaction history memory measure which memorizes a transaction history, and a notice transmitting means of transaction completion which transmits a notice of transaction completion which shows completion of dealings to said electronic money transaction device, A ******** computer and said electronic money transaction device, A history writing means which answers said notice of transaction completion from said notice transmitting means of transaction completion, and writes a transaction history in said 2nd memory measure, It has further a card balance update means adding said prescribed amount of money which said charge demand directs to the balance memorized by said 1st memory measure.

[0019]According to such composition, electronic money can be charged to an electronic money card, and various dealings can be conducted to it using charged electronic money. And since a transaction history is recorded on an added type storage parts store of a postscript, when abnormalities occur, a malfeasance etc. can be easily detected by verifying the contents of record of this added type storage parts store of a postscript. An ordinary savings account, a checking account, a loan account, credit account of a settlement account, etc. are arbitrary, and economic grounds which generate electronic money, such as whether it is pulling down from an account of the amount of money for correspondence or to be a loan, are arbitrary.

[0020]If said computer distinguishes whether it is said more than prescribed amount of money in which the balance (or loan limit) of said settlement account corresponding to this electronic money card is directed by said charge demand and this balance becomes in this less than prescribed amount of money, It may have a means to transmit an error message to said electronic money transaction device, and a means to stop dealings. The safety of dealings can be improved by having such composition.

[0021]For example, said 1st memory measure of said electronic money card is constituted by IC chip provided with a memory, and said 2nd memory measure is constituted by storage which is not rewritable.

[0022]Said transaction history may also contain said card identity numerals of said electronic money card, and said terminal identification numerals of said electronic money transaction device. According to this composition, a card and a terminal in which a malfeasance etc. were performed can be specified. Information for specifying this electronic money card may be removed from a transaction history recorded on said electronic money card. The electronic money card is always being used for a transaction history registered into each electronic money card. Therefore, it is satisfactory even if it removes this data.

[0023]Said transaction history is provided with the following.

For example, a dealings date.

Said terminal identification numerals of said electronic money transaction device which transmitted said charge demand.

Transaction money amount.
Dealings can be followed using these information.
[0024]Said 2nd memory measure of said electronic money card memorizes a transaction history of all the dealings dealt with with this electronic money card, for example. Said transaction history memory measure of said computer records a transaction history of all the dealings dealt with with said electronic money card, for example. By having such composition, dealings can be followed correctly. An unjust generation place etc. can be easily distinguished by comparing a transaction history stored in an electronic money card, and a transaction history stored in a computer.
[0025]An invalid card, an accident terminal, etc. in which use is not permitted are registered into a computer, and it may be made to forbid dealings when these cards or terminals are used.
[0026]A certificate authority for distinguishing whether an electronic money card is registered as an usable thing with this electronic money system may be arranged. This certificate authority distinguishes whether an individual public key and card identity numerals of an electronic money card are registered beforehand, for example.
[0027]Said electronic money card is provided with an individual public key and an individual secret key of a couple, and said electronic money transaction device, Have a terminal public key and a terminal secret key of a couple, and said charge demand, Information about dealings, and the 1st attestation child generated using said individual secret key, it is distinguished whether the said 1st and 2nd attestation child of said computer corresponds using said individual secret key and said terminal secret key including information about said dealings, the 2nd attestation child generated using said terminal secret key, said individual public key, and said terminal public key -- it may constitute like. When injustice is performed by one side of an electronic money card and an electronic money transaction device, the 1st attestation child and the 2nd attestation child stop being in agreement. Therefore, injustice can be distinguished.
[0028]Characteristic data in which an operator's bodily features is shown can be read, and it can be distinguished whether it is what has just authority based on this.
[0029]An electronic money system concerning the 3rd viewpoint of this invention, In an electronic money system which trades in electronic money using an electronic money card which stores electronic money which has a monetary value, said electronic money card, Have an added type storage parts store of a postscript, and an IC memory part, and an IC memory part, Memorize information for accessing information and said added type storage parts store of a postscript for specifying an electronic money card, and said electronic money system, It has a history recording device which remembers a history of dealings of electronic money conducted to an added type storage parts store of said electronic money card of a postscript by using this electronic money card to be a dealings means to trade in electronic money stored in said electronic money card. According to such composition, dealings of electronic money made with each electronic money card are recorded on an added type storage parts store of a postscript. An alteration of an added type storage parts

store of a postscript is difficult. Therefore, inaccurate existence etc. can be distinguished by following a transaction history recorded on an added type storage parts store of a postscript.

[0030]Said electronic money system may be provided with a history storage means which memorizes further a history of dealings of electronic money conducted with this electronic money system. By having such composition, injustice etc. can be followed more correctly and easily.

[0031]An electronic money system concerning the 4th viewpoint of this invention equips with the following an electronic money system which trades in electronic money using a medium by which electronic money information is recorded.

A reading means which reads characteristic data about a user's bodily features currently recorded on a medium.

A scanning means which scans the whole or a part of a card user's body.

A means to change data scanned by said scanning means into form of data currently recorded on said medium, A scanning means which compares data after conversion with data currently recorded on a medium, a means to judge the degree of coincidence by comparison of said data, and a means which validates an electronic money transaction when the above-mentioned decision result is beyond constant value.

According to such composition, an operator's justification is distinguished based on an operator's bodily features, and an unauthorized use can be prevented effectively.

[0032]An electronic money card which stores information concerning a monetary value in an electronic money system, Are a computer connected with two or more terminals which process this electronic money card, and a terminal of this plurality by a communication line, and an electronic money system constituted more, and said two or more terminals, An input means which inputs directions and transaction money amount of storing information about a monetary value in said electronic money card, A charge request means which transmits to said computer by making into a charge request message account specific information for specifying directions and transaction money amount which were inputted by said input means, and an account, A means by which a preparation and said computer receive said charge request message, With a means to memorize account specific information and transaction money amount which said charge request message which received shows as loan information, and to return a charge reply telegraphic message, said two or more terminals, It may constitute so that it may have a means to record transaction history information including information about a monetary value on said prepaid card, according to reception of said charge reply telegraphic message from said computer.

According to such composition, electronic money can be charged to an electronic money card, and various dealings can be conducted to it using charged electronic money.

[0033]Said computer may be further provided with an amount-of-money transportation device which moves said transaction money amount to a predetermined account from an account which said account specific information specifies based on said loan information.

[0034]A medium concerning the 6th viewpoint of this invention, Two or more terminals

which process an electronic money card which is provided with an added type storage parts store of a postscript, and an IC memory part for a computer, and stores information about a monetary value, It is the recording medium which recorded a program for making it function as said terminal in a system provided with a center connected with a terminal of this plurality by communication and in which computer reading is possible, Directions and transaction money amount which were inputted by input means which inputs directions and transaction money amount of storing information concerning a monetary value in this computer in said electronic money card, and said input means, A transmitting means which transmits account specific information for specifying an account to said center as a charge request message, Charge permission wording of a telegram which answered said charge request message and has been returned from said center is received, Position information which shows a position which should write in data is read from said IC memory part of said electronic money card, A program for making it function according to this position information by making transaction history information including information about said monetary value into a means written in said added type storage parts store of said electronic money card of a postscript is recorded. According to such composition, a terminal for charging electronic money is realizable for an electronic money card using the usual computer.

[0035]A medium concerning the 7th viewpoint of this invention, A computer, As an electronic money transaction device which processes an electronic money card which memorizes electronic money information and card identity numerals in an electronic money system for trading in electronic money which is the electronic information which has a monetary value, and a transaction history of electronic money. Are computer reading good signifier recording media to operate, and this computer, A charge request input means to input a charge demand which requires a supplement to said electronic money card of electronic money of prescribed amount of money, While answering a notice from said center answered and returned to a charge demand transmitting means which transmits said charge demand to a center, and said charge demand and recording a transaction history on said electronic money card, A program for considering it as a card renewal means to add said prescribed amount of money, and making it function on the balance memorized by this electronic money card is recorded. According to such composition, a terminal for charging electronic money is realizable for an electronic money card using the usual computer.

[0036]A medium concerning the 8th viewpoint of this invention, A scanning means which scans the whole or a part of a card user's body for a computer, A conversion method which changes into prescribed format data scanned by said scanning means, A reading means which reads characteristic data about a user's bodily features currently recorded on a medium by which electronic money information is recorded, When a means to compare data read by said reading means with data changed by said conversion method, a means to judge the degree of coincidence in comparison of said data, and the above-mentioned decision result are beyond constant value, a program for considering it as a means which

validates an electronic money transaction, and making it function is recorded.

[0037]

[Embodiment of the Invention]Hereafter, the electronic money system concerning this embodiment of the invention is explained with reference to drawings. This electronic money system is constituted more with the certificate authority 11 and the electronic money server 13 which are arranged at the center 10, the electronic money terminal (dealing device) 15, the bank center 17, and the electronic money card 19, as shown in drawing 1.

[0038]The center 10 is a computer system which controls operation of this whole electronic money system, and circulation of electronic money (management). The certificate authority 11 of the center 10 generates certification information to the user in this electronic money system, etc. It memorizes card ID and the public key of all the electronic money cards 19 which are used in this system in order to confirm that the user is registered, when the certificate authority 11 attests.

[0039]The certificate authority 11 generates and memorizes center secret key Ck1 of a couple, and center public key Ck2. The certificate authority 11 shares center secret key Ck1 within the center 10 by copying center secret key Ck1 to the electronic money server 13. The certificate authority 11 distributes center public key Ck2 to each electronic money terminal 15 grade beforehand via the electronic money server 13. The certificate authority 11 generates and memorizes the signature key Sk for generating the personal authentication information mentioned later, and the check key Ek for checking the signature made by the signature key Sk, i.e., personal authentication information, and distributes the check key Ek to each electronic money terminal 15 beforehand.

[0040]The balance table showing the balance of the electronic money which each electronic money card 19 holds as the electronic money server 13 is shown in drawing 2 and drawing 3, The list (invalid card list) of card ID of the electronic money card 19 whose use became improper, the list (accident terminal list) of terminal ID of the electronic money terminal 15 whose use became improper, and the list of histories of dealings of electronic money (transaction history table) are memorized.

[0041]The electronic money server 13 performs control, management, etc. of the authentication demand to the certificate authority 11, the change demand to the bank center 17, each electronic money card 19, and the electronic money terminal 15 using these stored data in order to trade in electronic money.

[0042]The electronic money terminal 15 is a terminal for trading in electronic money by a user's inserting or carrying the electronic money card 19, and carrying out predetermined operation. The charge terminal (ATM etc.) for supplementing the electronic money terminal 15 with electronic money at the electronic money card 19 (charge), It is arranged at the terminal which processes transfer of the electronic money between electronic money cards, a store, etc., and there are a POS terminal, a vending machine, etc. which receive the electronic money equivalent to an article or the amount of proceeds of service. It may have two or more functions, for example, an ATM function and a POS function, in which

one terminal is related with electronic money.
[0043]Each electronic money terminal 15 is provided with the following.
Storage parts store 30.
Input part 31.
Indicator 32.
Card processing part 33.

[0044]The storage parts store 30 stores the transaction history etc. of the electronic money at the time of the off-line of the check key Ek for a personal authentication information check and center public key Ck2 and terminal public key Tk2 [terminal secret key Tk1 of a couple and] which were supplied from terminal ID given to the electronic money terminal 15 and the above-mentioned certificate authority 11, and the center 10.
[0045]The input part 31 inputs directions of an electronic money transaction. The indicator 32 displays a processing menu, a message, etc. The card processing part 33 is provided with the following.
The loading slot which receives the electronic money card 19.
The IC lead / light part for accessing IC part 20 of the electronic money card 19
The optical memory read/write part for accessing the optical storing part 21.

[0046]The example of the ATM type electronic money terminal 15 is shown in drawing 4 (A). The input part 31 and the indicator 32 of this electronic money terminal 15 comprise the touch-panel type indicator 34, and the card processing part 33 is provided with the card slots 35A and 35B in which the electronic money card 19 is inserted. As for the card slot 35A, the card of the usual processing and transfer origin in the case of transfer of electronic money is inserted. The card of the transfer place in the case of transfer of electronic money is inserted in the card slot 35B.
[0047]The example of a POS type electronic money terminal is shown in drawing 4 (B). The input part 31 of this electronic money terminal 15 contains the keyboard 31A, the bar code reader 31B, etc. for selling with directions of dealings of electronic money, etc. and inputting the amount of the amount of money, etc. The indicator 32 is sold with a message etc. for an electronic money transaction, displays the amount of money etc., and is provided with the indicator 32A for customers, and the indicator 32B for operators. The card processing part 33 is provided with the card slot 35. The money drawer 36 grade is also arranged for POS.
[0048]The bank center 17 is provided with the exception stage account which are a settlement account which is an account of the user (carrier) of the electronic money card 19, and an employment account of the electronic money which a bank holds, and performs cash-receipt-and-disbursement processing of these accounts. for example, -- from the settlement account corresponding to [according to the directions from the center 10] the electronic money card 19 in the bank center 17 -- specially -- the change to an account -- and change from an account to a settlement account is performed specially. In order to

perform this change processing, the bank center 17 memorizes the account table to which the account number of the settlement account of the user (carrier) of card ID given to each electronic money card 19 and each electronic money card 19 is made to correspond, as shown in drawing 5.

[0049]The electronic money card 19 comprises an optical IC hybrid card provided with IC part (IC chip) 20 and the optical storing part 21, as shown in drawing 6. What is necessary is just to have IC part (IC chip) 20 and the optical storing part 21, and the shape is not limited to a card shape, but that of the electronic money card 19 is arbitrary.

[0050]IC part 20 builds in a control circuit and a memory circuit. This memory circuit memorizes card ID and individual secret key Pk1, individual public key Pk2, the balance of electronic money, personal authentication information for online trades mentioned later, etc. other than an operation program, as shown in drawing 6. IC part 20 memorizes the last dealings pointer in which the position of a final transaction history is shown among the transaction histories memorized by the optical storing part 21 mentioned later, and the transmitted pointer in which the position of the transaction history which transmitted to the electronic money server 13 at the end is shown.

[0051]By irradiating light energy, the optical storing part 21 comprises an added-a postscript type storage etc. which cannot rewrite the type with which a pit etc. are formed and data is written in, and memorizes the transaction history of the electronic money dealt with with the electronic money card 19 one by one, for example.

[0052]Use classification which shows the classification of dealings of electronic money as an item which constitutes a transaction history 0 [charge and (supplement of the balance)] Terminal ID of the electronic money transaction terminal 15 in which it was equipped with the electronic money card for dealings, such as payment, transfer, and liquidation, In transfer of the electronic money between the electronic money cards 19, a partner's card ID, There are a use date, transaction money amount, an attestation child (customer attestation child who created using secret key Pk1 of the above-mentioned item, the dealings attestation child and the above-mentioned item which were created using individual secret key Pk1, and business contacts (the electronic money terminal 15 or other electronic money cards 19)), etc.

[0053]In fundamental processing in the electronic money system which has such composition. (1) There are electronic money charge processing (supplement of the balance memorized by the electronic money card 19), (2) personal-authentication information issuing processing, (3) electronic-money-payment processing, (4) comparison processing, (5) electronic-money transfer processing, (6) electronic-money liquidation processing, etc. These processings are explained to turn below.

[0054](1) Explain electronic money charge processing electronic money charge processing with reference to drawing 7. The electronic money terminal 15 provided with an ATM function shows the processing selection menu, as shown in drawing 8 (A). A user chooses "1 Charge of electronic money" from the processing menus currently displayed on the indicator 32 (touch panel 34).

[0055]This selection is answered, and the electronic money terminal 15 displays the message of the purport that the electronic money card 19 should be inserted in the card slot 35A, as shown in drawing 8 (B).

[0056]If the electronic money card 19 is inserted, the electronic money terminal 15 will display the amount input screen of charge money as shown in drawing 8 (C), and a user will input the desired amount of charge money from the input part 31 (touch panel 34). When the amount of charge money is inputted, the electronic money terminal 15, While transmitting the transaction information and terminal ID which comprise dealings classification (charge), a use date, and transaction money amount (amount of charge money) to the electronic money card 19, the requirement signal which requires card ID and transmission of individual public key Pk2 is transmitted (P1).

[0057]IC part 20 of the electronic money card 19 adds card ID to terminal ID and transaction information, These information is changed into a dealings attestation child {Pk1 (terminal ID+ transaction information + card ID)} using individual secret key Pk1, and the dealings attestation child and card ID, and individual public key Pk2 are transmitted to the electronic money terminal 15 (P2).

[0058]The electronic money terminal 15 uses transaction information, terminal ID ****, and terminal secret key Tk1 for card ID which received, and creates a customer attestation child {Tk1 (terminal ID+ transaction information + card ID)}. The customer attestation child {Tk1 (terminal ID+ transaction information + card ID)} who created the electronic money terminal 15, It points to charge of the demanded amount of money, and the charge request message containing terminal public key Tk2, card ID of the electronic money card 19, individual public key Pk2, and a dealings attestation child are transmitted to the electronic money server 13 (P3). A charge request message contains terminal ID of the electronic money terminal 15 of a transmitting agency.

[0059]The electronic money server 13 distinguishes whether card ID and terminal ID which received are registered into the invalid card list (drawing 2 (B)) and accident terminal list (drawing 2 (C)) which have been memorized to the storage parts store 30. When card ID and terminal ID which received were not registered into these lists and they are distinguished, the electronic money server 13 changes a dealings attestation child {Pk1 (terminal ID+ transaction information + card ID)} into terminal ID, transaction information, and card ID using individual public key Pk2 which received. A customer attestation child {Tk1 (terminal ID+ transaction information + card ID)} is changed into terminal ID, transaction information, and card ID using terminal public key Tk2 which received. It is distinguished whether terminal ID, the transaction information and card ID which were changed by the dealings attestation child, and terminal ID and transaction information which were changed by the customer attestation child, and card ID are in agreement. when these are in agreement, this dealings attestation child and a customer attestation child distinguish the electronic money server 13 from the right, and it moves the amount of money of the bank center 17 directed specially to the account from the settlement account corresponding to that card ID -- it needs (money is invested) -- the

payment wording of a telegram to direct is transmitted to the bank center 17 (P4).

[0060]When at least one side of card ID which received, and terminal ID is registered into the invalid card list and the accident terminal list, Or when at least a part of terminal ID, the transaction information, and card ID which were changed by the dealings attestation child and the customer attestation child are not in agreement, the electronic money server 13, The message which directs a charge failure is transmitted to the electronic money terminal 15, and a message indicator etc. inform an administrator etc. of unjust detection. The electronic money terminal 15 displays the message of the purport that charge is impossible on the indicator 32.

[0061]The bank center 17 will distinguish the account number corresponding to card ID from the electronic money server 13 with reference to the account table shown in drawing 5, if payment wording of a telegram is received. Next, the balance of the settlement account of this account number is checked, and it is distinguished whether it is more than the amount of money the balance was instructed to be. When it distinguishes that it is more than the amount of money the balance was instructed to be, it distinguishes that payment is possible and the prescribed amount of money specially directed to the account from the settlement account is moved (P(it changes) 5). Next, the completion wording of a telegram of payment which notifies change completion is transmitted to the electronic money server 13 (P6).

[0062]When money cannot be invested with shortage of the balance of a settlement account, the bank center 17 transmits the wording of a telegram which directs a charge failure to the electronic money server 13. The electronic money server 13 stops charge processing, and it transmits the same message as the electronic money terminal 15. The electronic money terminal 15 answers this message, and displays the message which shows that on indicator 32 grade.

[0063]If the electronic money server 13 receives the completion wording of a telegram of payment from the bank center 17, card ID [of the electronic money card 19] and individual public key Pk2 memorized to the storage parts store 30 will be transmitted to the certificate authority 11, and the certification information over them will be required (P7). The certificate authority 11 confirms whether card ID and individual public key Pk2 which received is registered into the list of card ID [which self memorizes], and individual public key Pk2. If they are registered, the certificate authority 11 will change card ID and individual public key Pk2 which received into certification information {Ck1 (card ID+Pk2)} using center secret key Ck1, and will return it to the electronic money server 13 with the completion wording of a telegram of attestation (P8).

[0064]The electronic money server 13 will update the balance data in which the balance of the electronic money charged by the electronic money card 19 is shown on the balance table shown in drawing 2 (A), if the completion wording of a telegram of attestation and certification information {Ck1 (card ID+Pk2)} are received. As shown in drawing 3, this transaction history that comprises transaction information (use classification (charge), a use date, transaction money amount), card ID, terminal ID, and an attestation child (a

dealings attestation child and customer attestation child) is added to the past transaction history, and is memorized. Next, the electronic money server 13 gives the certification information from the certificate authority 11 to this transaction history, and transmits to the electronic money terminal 15 with the completion wording of a telegram of charge which shows completion of charge (P9).

[0065]If a transaction history and certification information are received, using center public key Ck2, the electronic money terminal 15 will change certification information into card ID and individual public key Pk2, and will check it. If it checks that the certification information is a right thing, based on the received transaction history, the balance currently recorded on the memory area of IC part 20 will be updated via the control section of IC part 20.

[0066]The electronic money terminal 15 reads the last dealings pointer from IC part 20, To the next address position of the position which the last dealings pointer directs, this transaction history {transaction information (use classification (charge), use date, transaction money amount), card ID, terminal ID, and attestation child (dealings attestation child and customer attestation child)} is added to the past transaction history, and is memorized. The electronic money terminal 15 is updated so that the position of the transaction history which the last dealings pointer and the transmitted pointer which are recorded on the memory area of IC part 20 added may be pointed out via the control section of IC part 20 (P10). Then, the terminal 15 displays on the indicator 32 that charge was completed, and it discharges the electronic money card 19.

[0067]The case where the user A charges the electronic money of 10,000 cyclotomies for this electronic money charge processing to the self electronic money card 19A (card ID"C99") using the electronic money terminal 15B (terminal ID"T150") is explained to an example with reference to drawing 9. First, the user A chooses "1 Charge of electronic money" from the processing menu displayed on the indicator 32, inserts the electronic money card 19A in the electronic money terminal 15B, and inputs "10,000 yen" as the amount of charge money.

[0068]The electronic money terminal 15B answers this input, and transmits the transaction information and terminal ID"T150" which comprise dealings classification (charge), a use date, and transaction money amount to the electronic money card 19A with the requirement signal which requires card ID and individual public key Pk2 (L1).

[0069]The electronic money card 19A adds card ID"C99" to terminal ID"T150" and transaction information which were received, and creates a dealings attestation child {Pk1A (T150+ transaction information +C99)} using individual secret key Pk1A. The electronic money card 19A transmits the dealings attestation child {Pk1A (T150+ transaction information +C99)} who created to the electronic money terminal 15B with card ID"C99" and individual public key Pk2A (L2).

[0070]The electronic money terminal 15B adds terminal ID to the transaction information memorized to card ID"C99" and the storage parts store 30, and creates a customer attestation child {Tk1B (T150+ transaction information +C99)} using terminal secret key

Tk1B. The customer attestation child {Tk1B (T150+ transaction information +C99)} who created the electronic money terminal 15B, The charge request message which charge of the electronic money of 10,000 cyclotomies is required, and contains terminal ID"T150" and terminal public key Tk2B, Card ID"C99" of the electronic money card 19A, individual public key Pk2A, and a dealings attestation child {Pk1A (T150+ transaction information +C99)} are transmitted to the electronic money server 13 (L3).

[0071]The electronic money server 13 checks the unauthorized use of the electronic money terminal 15 and the electronic money card 19, when terminal ID"T150" and card ID"C99" which received distinguish whether it registers with the accident terminal list and the invalid card list.

[0072]If the electronic money card 19A and the electronic money terminal 15B are not any of an invalid card and an accident terminal, either and it will be distinguished as a result of a check, the electronic money server 13 will change a dealings attestation child into terminal ID, transaction information, and card ID using individual public key Pk2A. A customer attestation child is changed into terminal ID, transaction information, and card ID using terminal public key Tk2B. Subsequently, it is distinguished whether terminal ID, the transaction information and card ID which were changed by the dealings attestation child, and terminal ID and transaction information which were changed by the customer attestation child, and card ID are in agreement. When these are in agreement, this dealings attestation child and a customer attestation child distinguish the electronic money server 13 from the right, and it transmits the payment wording of a telegram it is directed to the bank center 17 that moves 10,000 yen to an account specially of the bank center 17 from the settlement account of card ID"C99" (L4).

[0073]/when it is distinguished that both or one side of the electronic money card 19A and the electronic money terminal 15B is an invalid card or an accident terminal. Or when terminal ID, the transaction information, and card ID which were changed by the dealings attestation child and the customer attestation child are not mutually in agreement, the electronic money server 13 transmits the message of the purport that it is unchargeable to the electronic money terminal 15B, and it notifies an administrator of detection of inaccurate or abnormalities.

[0074]The bank center 17 searches card ID"C99 "account number of settlement account" 30000001" with reference to the account table shown in drawing 5 when payment wording of a telegram is received, and the balance of an applicable account number distinguishes whether it is 10,000 yen or more of the directed amount of charge money. When the balance is less than 10,000 yen, the bank center 17 transmits the wording of a telegram of an unchargeable-because of insufficient funds purport to the electronic money server 13. the case where the balance is 10,000 yen or more -- the bank center 17 -- a settlement account -- "30000001" to the bank center 17 -- 10,000 yen is specially moved to an account and the completion wording of a telegram of payment is transmitted to the electronic money server 13 (L5).

[0075]The electronic money server 13 will transmit the attestation grant demand which

requires attestation from card ID of the electronic money card 19A, and individual public key Pk2A to the certificate authority 11 with card ID"C99" and individual public key Pk2A, if the completion wording of a telegram of payment is received from the bank center 17 (L6).

[0076]a certificate authority -- 11 -- self -- memorizing -- **** -- an electronic money card -- 19 -- A -- a card -- ID -- and -- an individual -- a public key -- Pk -- two -- a list -- having received -- a card -- ID"C -- 99 -- " -- an individual -- a public key -- Pk -- two -- A -- existing -- things (that is, it registers with the certificate authority 11) -- checking . When card ID"C99" and individual public key Pk2A are registered into the certificate authority 11, the certificate authority 11, The certification information {Ck1 (C99+Pk2A)} over card ID"C99" and individual public key Pk2A which received is generated using center secret key Ck1, and it transmits to the electronic money server 13 with the completion wording of a telegram of attestation which shows completion of attestation (L7).

[0077]if the electronic money server 13 receives the completion wording of a telegram of attestation -- use classification -- "charge", a use date and card ID"C99", terminal ID"T150", and the amount of charge money -- as a dealings attestation child, a customer attestation child, etc. generate a transaction history and "10,000 yen" are shown in drawing 3, it memorizes. It adds to the balance of 10,000 yen of card ID"C99" of the balance table shown in drawing 2 (A). The certification information from the certificate authority 11 is given to the generated transaction history, and it transmits to the electronic money terminal 15B with the completion wording of a telegram of charge (L8).

[0078]If the transaction history to which certification information was given is received, using center public key Ck2, the electronic money terminal 15B will change certification information {Ck1 (C99+Pk2A)} into card ID"C99" and individual public key Pk2A, and will check it. If it checks that the certification information of the is a right thing, the received transaction history will be transmitted to IC chip 20 of the electronic money card 19A (L9). IC chip 20 adds 10,000 yen to the balance which self has memorized based on the received transaction history.

[0079]The electronic money terminal 15B is updated so that the transaction history to which the last dealings pointer was read from IC chip 20, the transaction history was added to the next position of the position which the last dealings pointer of the optical storing part 21 shows, and the last dealings pointer and the transmitted pointer were added may be shown. Then, the terminal 15B displays on the indicator 32 that charge was completed, and it discharges the electronic money card 19A. Such can be carried out and the user A can charge the electronic money of 10,000 cyclotomies to the self electronic money card 19A.

[0080](2) Explain personal authentication information issuing processing, next the issue processing (personal authentication information issuing processing) of the personal authentication information memorized by IC part 20 of the electronic money card 19. In the electronic money payment processing by the off-line mentioned later, the electronic money card 19 shows the electronic money terminal 15 this personal authentication information, and it is receiving the check of that personal authentication information with

the electronic money terminal 15, and it becomes possible to trade. Since it is created based on card ID [of the electronic money card 19], and individual public key Pk2, personal authentication information needs to be acquired whenever individual secret key Pk1 and individual public key Pk2 are changed.

[0081]The schematic diagram of personal authentication information issuing processing is shown in drawing 10. First, as shown in drawing 8, "4 Issue of personal authentication information" is chosen from the processing menu displayed on the indicator 32, and the electronic money card 19 is inserted in the electronic money terminal 15. The electronic money terminal 15 answers this operation, and transmits the requirement signal which shows card ID and the demand of individual public key Pk2 to IC part 20 of the electronic money card 19 (P11).

[0082]Answering this requirement signal, IC chip 20 of the electronic money card 19 transmits card ID and individual public key Pk2 to the electronic money terminal 15 (P12). The electronic money terminal 15 transmits card ID and individual public key Pk2 which received to the electronic money server 13 with the certification information issue requesting which requires personal authentication information (P13). Certification information issue requesting contains terminal ID.

[0083]The electronic money server 13 will confirm whether card ID and terminal ID which received are registered into the invalid card ID list and the accident terminal ID list, if card ID, individual public key Pk2, and certification information issue requesting are received from the electronic money terminal 15.

[0084]When at least one side of card ID which received, and terminal ID is registered into the invalid card ID list or the accident terminal ID list as a result of the check, the electronic money server 13, The message of a purport which cannot publish personal authentication information is transmitted to the electronic money terminal 15, and a message indicator etc. inform an administrator of unjust detection. The electronic money terminal 15 displays this message.

[0085]When card ID and terminal ID which received are not registered into an invalid card ID list and an accident terminal ID list, the electronic money server 13 transmits the issue requesting (personal authentication information issuing demand) of card ID and individual public key Pk2 which received, and personal authentication information to the certificate authority 11 (P14).

[0086]The certificate authority 11 by referring to the list of card ID which self memorizes, and individual public keys, if card ID, individual public key Pk2, and a personal authentication information issuing demand are received from the electronic money server 13, It is confirmed whether card ID and the individual public key which were received are registered as an usable thing in this system. When not registered, the certificate authority 11 transmits wording of a telegram to that effect to the electronic money server 13. The electronic money server 13 transmits the same wording of a telegram as the electronic money terminal 15. The electronic money terminal 15 displays this message.

[0087]On the other hand, when card ID and individual public key Pk2 which received are

registered, the certificate authority 11 generates personal authentication information {Sk (card ID+Pk2)} using the signature key Sk for personal authentication information generation, and transmits to the electronic money server 13 with the completion wording of a telegram of issue (P15).

[0088]The electronic money server 13 transmits the personal authentication information {Sk (card ID+Pk2)} and the completion wording of a telegram of issue from the certificate authority 11 to the electronic money terminal 15 (P16). The electronic money terminal 15 transmits the received personal authentication information {Sk (card ID+Pk2)} to IC part 20 of the electronic money card 19 (P17). IC part 20 memorizes the received personal authentication information {Sk (card ID+Pk2)} to a store circuit. Then, the electronic money terminal 15 displays on the indicator 32 that acquisition of personal authentication information was completed, and it discharges the electronic money card 19.

[0089]The case where the user A acquires the personal authentication information on the electronic money card 19A (card ID"C99") for this personal authentication information issuing processing, for example is explained to an example with reference to drawing 11.

[0090]First, the user A chooses "4 Issue of personal authentication information" from the menus displayed on the indicator 32, and inserts the electronic money card 19A in the electronic money terminal 15B. The electronic money terminal 15B answers this operation, and transmits the requirement signal which requires transmission of card ID and an individual public key of the electronic money card 19A (L11).

[0091]IC part 20 of the electronic money card 19A will transmit card ID"C99" and individual public key Pk2A to the electronic money terminal 15B, if the requirement signal from the electronic money terminal 15B is received (L12). The electronic money terminal 15B transmits card ID"C99" and individual public key Pk2A which received to the electronic money server 13 with certification information issue requesting (L13).

[0092]The electronic money server 13 checks the unauthorized use of the electronic money card 19 and the electronic money terminal 15, when card ID"C99" and individual public key Pk2A which received distinguish whether it registers with the invalid card ID list and the accident terminal ID list. When distinguished from an unauthorized use, the electronic money server 13 transmits the message of a purport which cannot publish personal authentication information to the electronic money terminal 15B, and it notifies an administrator of unjust detection by a message indicator etc. The electronic money terminal 15B displays this message.

[0093]If usable [in the electronic money card 19A and the electronic money terminal 15B] as a result of a check, card ID"C99" and individual public key Pk2A will be transmitted to the certificate authority 11 with a personal authentication information issuing demand (L14).

[0094]By using the signature key Sk for card ID"C99" and individual public key Pk2A which received from the electronic money server 13, and giving a digital signature, the certificate authority 11 generates personal authentication information {Sk (C99+Pk2A)}, and transmits to the electronic money server 13 with the completion wording of a telegram

of issue (L15).

[0095]The electronic money server 13 transmits the personal authentication information {Sk (C99+Pk2A)} and the completion wording of a telegram of issue from the certificate authority 11 to the electronic money terminal 15 (L16). The electronic money terminal 15 transmits the personal authentication information received from the electronic money server 13 to the electronic money card 19A (L17). IC part 20 of the electronic money card 19A memorizes the personal authentication information received from the electronic money terminal 15. Then, the electronic money terminal 15B displays on the indicator 32 that acquisition of personal authentication information was completed, and it discharges the electronic money card 19A.

[0096]Personal authentication information may be automatically acquired via this electronic money terminal 15, when individual secret key Pk1 and individual public key Pk2 are changed with the electronic money terminal 15.

[0097](3) Explain electronic money payment processing, next electronic money payment processing with reference to drawing 12. This processing is processing for purchasing goods, service, etc. at a store etc. and, for example, paying that fee with electronic money. The electronic money terminal 15 takes the gestalt of a POS terminal as shown in drawing 4 (B), a vending machine, etc., for example.

[0098]For example, after selling with the POS terminal type electronic money terminal 15 and calculating a frame, the message of the purport that the method of paying is chosen is displayed on the indicator 32. Here, if the payment by an electronic money card is chosen, directions of the purport that the electronic money card 19 is inserted will be displayed, and the electronic money card 19 will be inserted in the electronic money terminal 15.

[0099]Transaction information and terminal ID which the electronic money terminal 15 answers insertion of the electronic money card 19, and comprise dealings classification, a use date, and transaction money amount (amount of a payment), The requirement signal which requires transmission of card ID, individual public key Pk2, personal authentication information {Sk (card ID+Pk2)}, and the balance is transmitted to the electronic money card 19 (P21).

[0100]IC part 20 of the electronic money card 19 adds card ID to terminal ID and transaction information which were received, and creates a dealings attestation child {Pk1 (terminal ID+ transaction information + card ID)} using individual secret key Pk1. IC part 20 transmits card ID, individual public key Pk2, and personal authentication information {Sk (card ID+Pk2)} and the balance for the dealings attestation child {Pk1 (terminal ID+ transaction information + card ID)} who created to the electronic money terminal 15 (P22).

[0101]If card ID, individual public key Pk2, personal authentication information {Sk (card ID+Pk2)} and the balance, and a dealings attestation child {Pk2 (terminal ID+ transaction information + card ID)} are received from the electronic money card 19, the electronic money terminal 15, First, personal authentication information {Sk (card ID+Pk2)} is changed into card ID and individual public key Pk2 using the check key Ek, and these distinguish whether it is in agreement with card ID and individual public key Pk2 which

received from the electronic money card 19. When not in agreement, it judges that the electronic money terminal 15 has some injustice, a message [that it cannot trade] is displayed, and unjust detection is notified to the electronic money server 13.

[0102]If it judges that the electronic money terminal 15 is in agreement with card ID decoded from personal authentication information, card ID which individual public key Pk2 received from the electronic money card 19, and individual public key Pk2, it will be distinguished whether the balance which received is more than an amount paid. If the balance becomes in more than the amount of a payment, it will judge that payment is possible and a customer attestation child {Tk1 (terminal ID+ transaction information + card ID)} will be generated using terminal secret key Tk1 to transaction information, card ID, and terminal ID. The electronic money terminal 15 constitutes a transaction history from transaction information, card ID, terminal ID, a dealings attestation child {Pk2 (terminal ID+ transaction information + card ID)}, and a customer attestation child {Tk1 (terminal ID+ transaction information + card ID)}, It transmits to the electronic money card 19 with payment completion wording of a telegram (P23), and memorizes also to the storage parts store 30 of further self.

[0103]IC part 20 of the electronic money card 19 updates the balance stored in a store circuit based on the received transaction history, and it transmits the value of the last history pointer to the electronic money terminal 15. The electronic money terminal 15 writes a transaction history in the next address of the address which the last history pointer of the optical storing part 21 of the electronic money card 19 directs, and it sends out the command which updates the last history pointer to IC part 20. Answering this command, IC part 20 updates the value of the last dealings pointer stored in the store circuit. However, the value of a transmitted pointer is not updated. Then, the electronic money terminal 15 indicates that payment was completed, and it discharges the electronic money card 19.

[0104]As mentioned above, this electronic money payment processing is off-line processing processed between the electronic money card 19 and the electronic money terminal 15. By this, processing speed can be improved, a response can be made quick, and a customer's waiting time etc. can be shortened.

[0105]The electronic money terminal 15 communicates with the electronic money server 13 to predetermined timing, and transmits the transaction history which was being accumulated in the storage parts store 30. The electronic money server 13 memorizes the received transaction history on a transaction history table, as shown in drawing 3. As timing to which the electronic money terminal 15 transmits a transaction history to the electronic money server 13, the timing immediately after, for example, completing electronic money payment processing etc. is desirable. however -- responding to the polling from not the thing limited to this but every fixed time (every [for example,] 10 minutes) and the electronic money server 13 -- etc. -- it is arbitrary.

[0106]The electronic money terminal 15 may distinguish and manage a transmitted transaction history and an untransmitted transaction history by eliminating a transmitted

transaction history and giving a transmitted flag etc., after transmitting the transaction history which was being accumulated in the storage parts store 30 to the electronic money server 13.

[0107]The case where terminal ID purchases 10,000 yen goods at the store where the electronic money terminal 15B of "T150" was set up in electronic money payment processing, and the user A performs [the electronic money card 19A (card ID"C99")] the payment for example, is explained to an example with reference to drawing 13. first, the indicator 32 of the electronic money terminal 15B (for example, POS terminal) -- the amount of money -- "10,000 yen" are displayed as an amount paid and presupposes that the user chose the payment by electronic money. First, the user A or a salesclerk inserts the electronic money card 19A in the electronic money terminal 15B.

[0108]The electronic money terminal 15B answers insertion of the electronic money card 19A, The requirement signal which requires transmission of the transaction information and terminal ID"T150" which comprise dealings classification, a dealings date, and transaction money amount, card ID"C99", individual public key Pk2, personal authentication information, and the balance is transmitted to the electronic money card 19A (L21).

[0109]The electronic money card 19A adds card ID"C99" to terminal ID"T150" and transaction information which were received, and creates a dealings attestation child {Pk1A (T150+ transaction information +C99)} using individual secret key Pk1A. The electronic money card 19A transmits the dealings attestation child {Pk2A (T150+ transaction information +C99)} who created, card ID"C99", individual public key Pk2A, and personal authentication information {Sk (C99+Pk2)} and the balance to the electronic money terminal 15 (L22).

[0110]The electronic money terminal 15B receives card ID"C99", individual public key Pk2A, personal authentication information {Sk (card ID+Pk2)} and the balance, and a dealings attestation child {Pk1A (T150+ transaction information +C99)} from the electronic money card 19A, Personal authentication information {Sk (C99+Pk2)} is changed into card ID and individual public key Pk2A using the check key Ek memorized beforehand. Next, card ID and individual public key Pk2A which were decoded from personal authentication information check that it is in agreement with card ID"C99" of the electronic money card 19A, and individual public key Pk2A.

[0111]Next, the electronic money terminal 15B distinguishes whether the balance of the electronic money card 19A is more than the amount of a payment (in this case, 10,000 yen). If the balance of 10,000 yen or more becomes, the electronic money terminal 15B will generate a customer attestation child {Tk1B (T150+ transaction information +C99)} using terminal secret key Tk1B to terminal ID"T150", transaction information, and card ID"C99." A transaction history is constituted from terminal ID"T150", transaction information, card ID"C99", a dealings attestation child {Pk1A (T150+ transaction information +C99)}, and a customer attestation child {Tk1B (T150+ transaction information +C99)}, It transmits to the electronic money card 19A with payment

completion wording of a telegram (L23). A transaction history is memorized also to the self storage parts store 30. Then, the electronic money terminal 15B indicates that payment was completed, and it discharges the electronic money card 19A.

[0112]Based on the transaction history received from the electronic money terminal 15B, IC part 20 of the electronic money card 19A subtracts 10,000 cyclotomies of balances, and it transmits the value of the last dealings pointer to the electronic money transaction terminal 15B. The electronic money transaction terminal 15B stores a transaction history in the next address of the address which the last dealings pointer of the optical storing part 21 shows. Then, to IC part 20, the value of the last read pointer is updated so that the following address position may be shown. However, the value of a transmitted pointer is not updated.

[0113]When the electronic money terminal 15B, on the other hand, judges that card ID and individual public key Pk2 which were changed from personal authentication information {Sk (card ID+Pk2)} are not in agreement with card ID"C99" of the electronic money card 19A, and individual public key Pk2A, The electronic money terminal 15B distinguishes the electronic money card 19A from a wrong card, pays it, and displays the message of an improper purport on the indicator 32, and it notifies unjust detection to the electronic money server 13. When the balance of the electronic money card 19A is less than 10,000 yen, the electronic money terminal 15B is paid because of insufficient funds, and displays the message of an improper purport on the indicator 32.

[0114]The electronic money terminal 15B transmits the transaction history memorized to the storage parts store 30 to the electronic money server 13 after the end of payment processing. If a transaction history is received, the electronic money server 13 stores the received transaction history in a transaction history table, as shown in drawing 3. The electronic money terminal 15B may distinguish and manage a transmitted transaction history and an untransmitted transaction history by eliminating a transmitted transaction history from the electronic money server 13 after the completion of transmitting of the transaction history which was being accumulated in the storage parts store 30 of the transaction history, and giving a transmitted flag etc.

[0115]In the above explanation, although payment processing was performed off-line, in order to raise security, when transaction money amount is more than a constant sum, it may be made to process on-line and 1 time of the amount of a trading limit may be defined.

[0116](4) Execution of comparison processing payment processing etc. will generate an untransmitted transaction history to the electronic money server 13 in the electronic money card 19. These transaction histories are transmitted to the electronic money server 13 in advance of the processing at the time of execution of the processings (for example, charge processing of electronic money etc.) performed on-line. The electronic money server 13 will check the justification by comparing with the transaction history which self has memorized, if a transaction history is received via the electronic money terminal 15 from the electronic money card 19. The outline of this comparison processing is explained with reference to drawing 14.

[0117]If the signal from the electronic money terminal 15 is received, IC part 20 of the electronic money card 19 will distinguish the contents of the processing which the received signal directs, and will distinguish whether it is pointing to on-line processing. When the input signal is pointing to on-line processing, IC part 20 distinguishes whether it is the no the value of the last dealings pointer and whose value of a transmitted pointer correspond, before performing other processings. When in agreement and it distinguishes, IC part 20 transmits the transaction history and card ID which are memorized to each address from the next position of the pointer which a transmitted pointer shows with an interrupt signal to the position which the last dealings pointer shows, and an individual public key to the electronic money terminal 15 (P31).

[0118]For example, when "charge processing of electronic money" is chosen from processing menus, the electronic money card 19 is inserted in the electronic money terminal 15 and the amount of money is inputted, the electronic money terminal 15, For example, in order to perform charge processing, transaction information etc. are transmitted to IC part 20 of the electronic money card 19 (L1 of drawing 7 P1 and drawing 9).

[0119]IC part 20 distinguishes from transaction information that the directed processing is on-line processing, and distinguishes whether it is the no whose last dealings pointer and transmitted pointer of IC part 20 correspond. When in agreement and it distinguishes, IC part 20 transmits the transaction history and card ID which are memorized to each address from the next position of the pointer which a transmitted pointer shows with an interrupt signal to the position which the last dealings pointer shows, and individual public key Pk2 to the electronic money terminal 15 (P31).

[0120]The electronic money terminal 15 answers an interrupt signal, and transmits card ID and individual public key Pk2 which received, and a transaction history to the electronic money server 13 (P32).

[0121]The electronic money server 13 transmits to the certificate authority 11 with the acknowledge request which requires the check of they being registered into the certificate authority 11 in card ID and individual public key Pk2 which received (P33).

[0122]The certificate authority 11 distinguishes whether card ID and individual public key Pk2 which received are registered into the list of card ID which self memorizes, and individual public keys. A check of being registered will return the completion wording of a telegram of a check which shows completion of a check to the electronic money server 13 (P34). When card ID and individual public key Pk2 which received are not registered, the certificate authority 11 notifies unjust detection to the electronic money server 13.

[0123]If the completion wording of a telegram of a check from the certificate authority 11 is received, the electronic money server 13 will compare the transaction history received from the electronic money card 19 with the transaction history which self has memorized. If all of the received transaction history and the transaction history which self has memorized are in agreement and comparison is completed, the electronic money server 13 will be compared to the electronic money terminal 15, and will transmit completion wording of a

telegram (P35).

[0124]The electronic money terminal 15 transmits the comparison completion wording of a telegram which received to the electronic money card 19 (P36). If comparison completion wording of a telegram is received, the electronic money card 19 will update the transmitted pointer memorized to IC part 20 so that it may be in agreement with the last dealings pointer. Then, processing originally demanded with the electronic money terminal 15 is performed.

[0125]When it is judged that the received transaction history and the transaction history of the electronic money server 13 which self has memorized do not correspond, compare to the electronic money terminal 15 and disagreement is notified, and a message indicator etc. inform an administrator etc. of unjust detection.

[0126]Since a non-transmission history does not exist when the last dealings pointer and a transmitted pointer are in agreement, the electronic money card 19 continues processing according to a requirement signal.

[0127]Only after electronic money payment processing is made, it may be made to perform this comparison processing. In this case, for example, the electronic money terminal 15 will set a non-transmission history flag to IC part 20 of the electronic money card 19, if electronic money payment processing is performed. If the electronic money card 19 is inserted and on-line processing is directed, the electronic money transaction terminal 15 distinguishes whether a non-transmission history flag is one, and if it is one, it will perform above-mentioned comparison processing.

[0128]This comparison processing is concretely explained with reference to drawing 15 and drawing 16. Here, before, the user A is making payment of electronic money with the electronic money card 19A of card ID"C99", and assumes that the untransmitted transaction history is memorized at the optical storing part 21 of the electronic money card 19A.

[0129]The user A points to charge of electronic money, and inserts the electronic money card 19A in the electronic money terminal 15B, for example. The electronic money terminal 15B transmits the transaction information which comprises dealings classification (charge), a use date, and transaction money amount, and terminal ID to IC part 20 of the electronic money card 19A with the requirement signal which requires card ID and individual public key Pk2.

[0130]It is distinguished whether the last dealings pointer which distinguished that on-line processing was chosen and has memorized it inside, and the transmitted pointer of IC part 20 correspond from transaction information. As shown in drawing 16, supposing a transmitted pointer points out address"2" and the last dealings pointer shows address"5", IC part 20, the address which the transmitted pointer has pointed out -- the next address of "2" -- the transaction histories R3-R5 to "address "5 which the last dealings pointer has pointed out from 3"" are transmitted to the electronic money terminal 15B with an interrupt signal, card ID"C99", and individual public key Pk2A (L31). The electronic money terminal 15B transmits the transaction histories R3-R5 and card ID which received,

and individual public key Pk2A to the electronic money server 13 (L32).

[0131]The electronic money server 13 transmits card ID"C99" and individual public key Pk2A which received to the certificate authority 11 with an acknowledge request (L33). The certificate authority 11 checks that card ID which self memorizes, card ID which received on the list of individual public keys, and individual public key Pk2A are registered, and transmits the completion wording of a telegram of a check to the electronic money server 13 (L34).

[0132]The electronic money server 13 will compare the transaction histories R3-R5 and the transaction history which self has memorized, if the completion wording of a telegram of a check is received. That is, the transaction histories R3-R5 of address"3"-"5" confirm that it is in agreement with the transaction history altogether memorized by the electronic money server 13. If the transaction histories R3-R5 are in agreement with the transaction history memorized by the electronic money server 13 as a result of a check, the electronic money server 13, The balance of card ID"C99" of the balance table shown in drawing 2 (A) is updated, it compares to the electronic money terminal 15B, and completion wording of a telegram is transmitted (L35). The electronic money terminal 15B transmits the comparison completion wording of a telegram which received to the electronic money card 19A (L36). If comparison completion wording of a telegram is received, the electronic money card 19A will update the transmitted pointer memorized to IC part 20 from "2" to "5", as shown in drawing 16.

[0133]Then, the electronic money terminal 15 and the electronic money card 19A perform electronic money charge processing directed.

[0134]The comparison processing mentioned above compares the transaction history from the electronic money terminal 15 memorized from the electronic money card 19 to a transaction history and the electronic money server 13. The transaction history (for example, transaction money amount was altered) generated unjustly by this is easily detectable. When injustice is detected, by referring to the transaction history memorized by the optical storing part 21 of the inaccurate electronic money card 19, when and where, it was used how much or the using history of ** can be known.

[0135](5) Explain the outline of transfer processing of electronic money, next electronic money transfer processing with reference to drawing 17. Use as the electronic money card 19A the side which transfers electronic money (move), and let the side which receives transfer be the electronic money card 19B.

[0136]"3 Transfer of electronic money" is chosen from the processing menu displayed on the indicator 32 according to a screen display shown in drawing 8, The electronic money card 19A is inserted in the card slot 35A, the electronic money card 19B is inserted in the card slot 35B, respectively, and the amount of money for transfer from the electronic money card 19A to the electronic money card 19B is inputted. Transaction information and terminal ID which the electronic money terminal 15 answers this input, and are constituted from dealings classification (transfer to 19B from 19A), a use date, and transaction money amount by the electronic money card 19A and the electronic money card

19B, The requirement signal which shows the demand of card ID and an individual public key is transmitted, respectively (P41).

[0137]The electronic money card 19A will create the dealings attestation child {Pk1A (card ID of terminal ID+ transaction information+19A)} to terminal ID, transaction information, and card ID of self using individual secret key Pk1A, if terminal ID and transaction information, and a requirement signal are received. The electronic money card 19A transmits the dealings attestation child and card ID which were created, and individual public key Pk2A to the electronic money terminal 15 (P42).

[0138]The electronic money card 19B will create the customer attestation child {Pk1B (card ID of terminal ID+ transaction information+19B)} to terminal ID, transaction information, and card ID of self using individual secret key Pk1B, if terminal ID and transaction information, and a requirement signal are received. The electronic money card 19B transmits the customer attestation child and card ID which were created, and individual public key Pk2B to the electronic money terminal 15 (P42).

[0139]The dealings attestation child {Pk1A (card ID of terminal ID+ transaction information+19A)} who received the electronic money terminal 15 from the electronic money card 19A, card ID, and individual public key Pk2A, The customer attestation child {Pk1B (card ID of terminal ID+ transaction information+19B)} who received from the electronic money card 19B, card ID, and individual public key Pk2B, The transfer request wording of a telegram it is directed that moves the amount of money (amount of money for transfer) inputted into the electronic money card 19B from the electronic money card 19A is transmitted to the electronic money server 13 (P43). Transfer request wording of a telegram contains terminal ID.

[0140]The electronic money server 13 distinguishes whether card ID and terminal ID of the electronic money card 19A and the electronic money card 19B which received are registered into the invalid card ID list and the accident terminal ID list.

[0141]When card ID and terminal ID which received are not registered into an invalid card ID list and an accident terminal ID list, the electronic money server 13 checks the balance of the electronic money card 19A of the balance table shown in drawing 2 (A). When the balance is insufficient, the message of the purport of insufficient funds is transmitted to the electronic money terminal 15. The electronic money terminal 15 displays the message of a purport which cannot transfer the directed amount of money because of insufficient funds.

[0142]When it is more than the amount of money for transfer the balance was instructed to be, the electronic money server 13 changes a dealings attestation child {Pk1A (card ID of terminal ID+ transaction information+19A)} into terminal ID, transaction information, and card ID of the electronic money card 19A using individual public key Pk2A of the electronic money card 19A. A customer attestation child {Pk1B (card ID of terminal ID+ transaction information+19B)} is changed into terminal ID, transaction information, and card ID of the electronic money card 19B using individual public key Pk2B of the electronic money card 19B. Next, it is distinguished whether the changed contents are the right.

Namely, the transaction information and terminal ID which were decoded from the dealings attestation child and the customer attestation child are in agreement, It is confirmed that card ID which card ID changed by the dealings attestation child changed from the customer attestation child in accordance with card ID of the electronic money card 19A of a transferring agency is in agreement with card ID of the electronic money card 19B of a transfer place. When in agreement altogether and it is distinguished, the balance of the electronic money card 19A of a balance table and the electronic money card 19B is updated, respectively.

[0143]Next, the electronic money server 13 transmits card ID and the individual public key of the electronic money card 19A and the electronic money card 19B to the certificate authority 11 with an attestation grant demand (P44).

[0144]It is confirmed whether the certificate authority 11 is registered into the list of card ID with which answer an attestation grant demand and self remembers card ID of the electronic money cards 19A and 19B which received and individual public key Pk2A, and Pk2B to be, and individual public keys. When it is judged that these are registered, using center secret key Ck1 to them Certification information {Ck1 (card ID+Pk 2A of 19A)}, {Ck1 (card ID+Pk2B of 19B)} is generated, respectively, and it transmits to the electronic money server 13 with the completion wording of a telegram of attestation (P45).

[0145]The electronic money server 13 answers the completion wording of a telegram of attestation, and generates and memorizes the transaction history of the electronic money card 19A of a transferring agency, and the transaction history of the electronic money card 19B of a transfer place. The certification information from the certificate authority 11 is added to those transaction histories, and it transmits to the electronic money terminal 15 with the completion wording of a telegram of transfer (P46).

[0146]If a transaction history and certification information are received, using center public key Ck2, the electronic money terminal 15 will change certification information into card ID and individual public key Pk2, and will check it. If it checks that the certification information is a right thing, the transaction history which answered the completion wording of a telegram of transfer, and was received will be transmitted to the electronic money card 19A and the electronic money card 19B, respectively (P47). IC part 20 of the electronic money cards 19A and 19B updates the balance which each has memorized based on the received transaction history. That is, IC part 20 of the electronic money card 19A carries out the prescribed-amount-of-money cut of the memorized balance based on the received transaction history, and IC part 20 of the electronic money card 19B carries out prescribed-amount-of-money increase of the memorized balance based on the received transaction history.

[0147]IC part 20 of the electronic money cards 19A and 19B transmits the value of the last dealings pointer to the electronic money terminal 15, respectively. The electronic money terminal 15 adds the transaction history received to the next address of the address which the value of the last dealings pointer of the optical storing part 21 of the electronic money cards 19A and 19B shows. It updates so that the transaction history to which the last

dealings pointer and the transmitted pointer were added may be shown. Then, the electronic money terminal 15C displays on the indicator 32 that transfer of electronic money was completed, and it discharges the electronic money cards 19A and 19B.

[0148]The user A this electronic money transfer processing from the electronic money card 19A (card ID"C99") to the electronic money card 19B (card ID"C05"). The case where the electronic money of 30,000 cyclotomies is transferred via the electronic money terminal 15C (terminal ID"T150") is explained to an example with reference to drawing 18.

[0149]First, according to a screen display shown in drawing 8, the user A chooses "3 Transfer of electronic money" from a processing menu, inserts the electronic money card 19A in the transferring agency card slot 35A, inserts the electronic money card 19B in the transfer place card slot 35B, and inputs the amount of money for transfer.

[0150]Answer this input and the electronic money terminal 15C, The requirement signal which shows the demand of card ID and an individual public key to the electronic money card 19A and the electronic money card 19B with the transaction information and terminal ID"T150" which comprise dealings classification, a use date, and transaction money amount is transmitted, respectively (L41).

[0151]The electronic money card 19A answers a requirement signal, and card ID"C99" of self is added to terminal ID"T150" and transaction information, A dealings attestation child {Pk1A (T150+ transaction information +C99)} is created using individual secret key Pk1A, and the dealings attestation child is transmitted to the electronic money terminal 15C with card ID"C99" and individual public key Pk2A (L42).

[0152]The electronic money card 19B answers a requirement signal, and card ID"C05" of self is added to terminal ID"T150" and transaction information, A customer attestation child {Pk1B (T150+ transaction information +C05)} is created using individual secret key Pk1B, and the customer attestation child is transmitted to the electronic money terminal 15C with card ID"05" and individual public key Pk2B (L42).

[0153]Card ID"C99", individual public key Pk2A, and the dealings attestation child {Pk1A (T150+ transaction information +C99)} who received the electronic money terminal 15C from the electronic money card 19A, Card ID"C05", individual public key Pk2B, and the customer attestation child {Pk1B (T150+ transaction information +C05)} who received from the electronic money card 19B, The transfer request wording of a telegram it is directed that moves 30,000 yen electronic money to the electronic money card 19B from the electronic money card 19A is transmitted to the electronic money server 13 (L43). Transfer request wording of a telegram contains terminal ID"T150."

[0154]electronic money -- a server -- 13 -- having received -- an electronic money card -- 19 -- A -- an electronic money card -- 19 -- B -- a card -- ID"C -- 99 -- " -- " -- C -- 05 -- " -- and -- a terminal -- ID"T -- 150 -- " -- an invalid card -- ID -- and -- an accident -- a terminal -- ID -- a list -- registering -- having -- **** -- ****** -- checking . When card ID"C99" and "C05" and terminal ID"T150" were not registered as an invalid card or an accident terminal and they are distinguished, the electronic money server 13 checks the balance of the electronic money card 19A of a transferring agency with reference to a balance table.

[0155]If the balance of less than 30,000 yen becomes, the electronic money server 13 will transmit the message of the purport of insufficient funds to the electronic money terminal 15. If the balance of 30,000 yen or more becomes, the electronic money server 13 will change a dealings attestation child {Pk1A (T150+ transaction information +C99)} into terminal ID, transaction information, and card ID of the electronic money card 19A using individual public key Pk2A. A customer attestation child {Pk1B (T150+ transaction information +C05)} is changed into terminal ID, transaction information, and card ID using individual public key Pk2B.

[0156]Then, it is distinguished whether these contents are the right. Namely, terminal ID and transaction information which were changed from the dealings attestation child and the customer attestation child are mutually in agreement, It is confirmed whether, in accordance with card ID"C99" of the electronic money card 19A of card ID's changed by dealings attestation child's transfer origin, card ID changed by the customer attestation child is in agreement with card ID"C05" of the electronic money card 19B of a transfer place. If a dealings attestation child and a customer attestation child are distinguished from the right as a result of a check, the electronic money server 13 will subtract the balance of only 30,000 yen of card ID"C99" in a balance table, and will add 30,000 yen to the balance of card ID"C05." Next, the electronic money server 13 transmits card ID"C99" [of the electronic money card 19A and the electronic money card 19B], "C05", and individual public key Pk2A, and Pk2B to the certificate authority 11 with an attestation grant demand (L44).

[0157]By the certificate authority's 11 answering an attestation grant demand, and referring to card ID and the public key which self memorizes, It is confirmed whether card ID"C99" [which received / of the electronic money card 19A and the electronic money card 19B], "C05", and individual public key Pk2A, and Pk2B are registered into this system. When it checks that they are registered, the certificate authority 11 Card ID"C99", The certification information {Ck1 (C99+Pk2A)} of the electronic money card 19A and the certification information {Ck1 (C05+Pk2B)} of the electronic money card 19B are generated using center secret key Ck1 to "C05" and individual public key Pk2A and Pk2B, respectively, It transmits to the electronic money server 13 with the completion wording of a telegram of attestation (L45).

[0158]If the certification information {Ck1 (C99+Pk2A)} of the electronic money card 19A and the electronic money card 19B and {Ck1 (C05+Pk2B)} are received, the electronic money server 13, The transaction history of the electronic money card 19A of a transferring agency and the transaction history of the electronic money card 19B of a transfer place are generated, and it memorizes on a transaction history table. The certification information from the certificate authority 11 is given to those transaction histories, and it transmits to the electronic money terminal 15C with the completion wording of a telegram of transfer (L46).

[0159]If a transaction history and certification information are received, using center public key Ck2, the electronic money terminal 15 will change certification information into

card ID and individual public key Pk2, and will check it. If it checks that the certification information is a right thing, the received transaction history will be transmitted to IC part 20 of the electronic money cards 19A and 19B, respectively (L47). IC part 20 of the electronic money cards 19A and 19B updates the balance memorized to the store circuit based on the received transaction history. That is, the electronic money card 19A reduces the balance of 30,000 yen, and the electronic money card 19B increases the balance of 30,000 yen. The electronic money terminal 15C reads the value of the last dealings pointer from IC part 20 of the electronic money cards 19A and 19B, and the last dealings pointer of the optical storing part 21 of the electronic money cards 19A and 19B adds a transaction history to the next address of the address which a value shows, respectively.

[0160]The terminal 15C is updated so that the transaction history to which the last dealings pointer and the transmitted pointer which are memorized by IC part 20 of the electronic money cards 19A and 19B were added may be shown. Then, the electronic money terminal 15C displays on the indicator 32 that transfer of electronic money was completed, and it discharges the electronic money cards 19A and 19B.

[0161]"3 Transfer of electronic money" is chosen from a menu, and when the amount of money for transfer is inputted, the electronic money terminal 15 may be made to perform the check of the balance of the electronic money card 19A of a transferring agency. In this case, the electronic money terminal 15 gives a balance demand to the electronic money card 19A.

[0162]In the above explanation, although transfer processing of electronic money was performed by on-line processing, when the amount of transfer is below a constant sum, the offline system processed within the electronic money terminal 15 may be adopted like electronic money payment processing. Thereby, response speed can be improved. In order to raise security in the case of off-line processing, the limit of 1 time of the amount of money for transfer may be defined.

[0163](6) Realize electronic money liquidation processing, next the electronic money accumulated in the electronic money card 19, and explain the outline of the electronic money liquidation processing transferred to a user's settlement account with reference to drawing 19. First, as shown in drawing 8, a user chooses "2 Liquidation of electronic money" from the processing menu displayed on the indicator 32, inserts the electronic money card 19 in the electronic money terminal 15, and inputs the amount of money for liquidation.

[0164]The electronic money terminal 15 answers this selection, and transmits the requirement signal which shows the demand of the transaction information and terminal ID which comprise dealings classification, a use date, and transaction money amount, card ID, and an individual public key to the electronic money card 19 (P51).

[0165]The electronic money card 19 answers a requirement signal, and card ID of self is added to terminal ID and transaction information, The dealings attestation child who created and created the dealings attestation child {Pk1 (terminal ID+ transaction information + card ID)} using individual secret key Pk1 is transmitted to the electronic

money terminal 15 with card ID and an individual public key (P52).

[0166]The electronic money terminal 15 adds transaction information and terminal ID to card ID which received, and creates a customer attestation child {Tk1 (terminal ID+ transaction information + card ID)} using terminal secret key Tk1. The customer attestation child {Tk1 (terminal ID+ transaction information + card ID)} who created the electronic money terminal 15, It points to shaking and changing to the inputted amount of money for liquidation, and a settlement account corresponding from the electronic money card 19, and the liquidation demand containing terminal public key Tk2, card ID of the electronic money card 19, and individual public key Pk2 are transmitted to the electronic money server 13 (P53). A charge request message contains terminal ID of the electronic money terminal 15 of a transmitting agency.

[0167]It is confirmed whether the electronic money server 13 is registered into the invalid card ID list in which self memorizes card ID and terminal ID of the electronic money card 19 which received, and the list of accident terminal ID. When card ID and terminal ID which received were not registered into an invalid card ID list and an accident terminal ID list and they are distinguished, the electronic money server 13, A dealings attestation child {Pk1 (terminal ID+ transaction information + card ID)} is changed into terminal ID, transaction information, and card ID using individual public key Pk2 which received. A customer attestation child {Tk1 (terminal ID+ transaction information + card ID)} is changed into terminal ID, transaction information, and card ID using terminal public key Tk2 which received, and it is distinguished whether these are in agreement. When these are in agreement, the electronic money server 13, A dealings attestation child {Pk1 (terminal ID+ transaction information + card ID)} and a customer attestation child {Tk1 (terminal ID+ transaction information + card ID)} distinguish from the right, and transmit card ID and individual public key Pk2 to the certificate authority 11 with an attestation grant demand (P54).

[0168]The certificate authority 11 confirms whether card ID and individual public key Pk2 which received are registered into the system by answering an attestation grant demand and referring to the list of card ID which self has memorized, and individual public keys. If they are registered, the certificate authority 11 will generate the certification information {Ck1 (card ID+Pk2)} over card ID and individual public key Pk2 which received using center secret key Ck1, and will transmit to the electronic money server 13 (P55). If card ID and individual public key Pk2 which received is not registered into a system, the certificate authority 11 will notify unjust detection to the electronic money server 13.

[0169]If certification information {Ck1 (card ID+Pk2)} is received from the certificate authority 11, the electronic money server 13 checks the balance of the electronic money card 19A with reference to a balance table, and if change is possible for it, The change request wording of a telegram containing card ID and transfer amount is created, and it transmits to the bank center 17 (P56).

[0170]When in agreement with either of the lists of card ID [that at least one side of card ID which received, and terminal ID cannot use it], and terminal ID, Or when terminal ID,

the transaction information, and card ID which were changed by the dealings attestation child and the customer attestation child are not mutually in agreement, the electronic money server 13 transmits the message of a purport [that it is unchargeable to the electronic money terminal 15], and it notifies an administrator of unjust detection by a message indicator etc. When the balance of the electronic money card 19 is insufficient, the electronic money server 13 transmits the message of the purport of insufficient funds to the electronic money terminal 15.

[0171]The bank center 17 will change the directed amount of money to the settlement account corresponding to card ID from an account specially with reference to the account table shown in drawing 5, if change request wording of a telegram is received (P57). The bank center 17 transmits change completion wording of a telegram to the electronic money server 13 after change completion (P58).

[0172]If change completion wording of a telegram is received, the electronic money server 13 will update the balance of the balance table of the electronic money card 19, will generate a transaction history, and will memorize it on a transaction history table. Next, the electronic money server 13 gives the certification information {Ck1 (card ID+Pk2)} from the certificate authority 11 to a transaction history, and transmits to the electronic money terminal 15 with the completion wording of a telegram of liquidation which shows that liquidation was completed (P59).

[0173]If a transaction history, and certification information {Ck1 (card ID+Pk2)} and change completion wording of a telegram are received, using center public key Ck2, the electronic money terminal 15 will change certification information {Ck1 (card ID+Pk2)} into card ID and individual public key Pk2, and will check it. If it checks that the certification information is a right thing, a transaction history will be transmitted to the electronic money card 19 (P60).

[0174]Based on the received transaction history, the IC card part 20 of the electronic money card 19 updates the balance, and it transmits the value of the last dealings pointer to the electronic money terminal 15. The electronic money terminal 15 is added to the next address of the address with which the last dealings pointer of the optical storing part 21 directs the received transaction history. Then, the last dealings pointer and the transmitted pointer which are memorized by the IC card part 20 are updated. Then, the electronic money terminal 15 displays on the indicator 32 that liquidation of electronic money was completed, and it discharges the electronic money card 19.

[0175]This electronic money liquidation processing among the electronic money which the user A has memorized to the electronic money card 19A (card ID"C99") 50,000 yen, The case where it changes to the self settlement account of the bank center 17 using the electronic money terminal 15B (terminal ID"T150") is explained to an example with reference to drawing 20. The user A chooses "2 Liquidation of electronic money" from the processing menu displayed on the indicator 32, equips the electronic money terminal 15B with the electronic money card 19A, and inputs the amount of money for liquidation "50,000 yen" into the input part 31.

[0176]Answering this operation, the electronic money terminal 15B transmits the transaction information constituted from dealings classification, a use date, and transaction money amount by the electronic money card 19A, terminal ID"T150", and the requirement signal which requires transmission of card ID and an individual public key (L51). an electronic money card -- 19 -- A -- a requirement signal -- answering -- having received -- a terminal -- ID"T -- 150 -- " -- and -- transaction information -- self -- a card -- ID"C -- 99 -- " -- adding -- an individual -- a secret key -- Pk -- one -- A -- using -- dealings -- attestation -- a child -- {-- Pk -- one -- A (T150+ transaction information +C99) --} -- creating . The electronic money card 19A transmits the dealings attestation child {Pk1A (T150+ transaction information +C99)} and card ID"C99" which were created, and individual public key Pk2A to the electronic money terminal 15B (L52).

[0177]The electronic money terminal 15B adds transaction information and terminal ID"T150" to card ID"C99" which received, and creates a customer attestation child {Tk1B (T150"+ transaction information +C99)} using terminal secret key Tk1. The customer attestation child {Tk1B (T150"+ transaction information +C99)} who created the electronic money terminal 15B, The liquidation demand which points to shaking and changing the inputted amount of money for liquidation to the settlement account corresponding to the electronic money card 19A from the electronic money card 19A, and contains terminal public key Tk2B, Card ID"C99" of the electronic money card 19A, individual public key Pk2A, and a dealings attestation child {Pk1A (T150"+ transaction information +C99)} are transmitted to the electronic money server 13 (L53).

[0178]The electronic money server 13 confirms whether card ID"C99" of the electronic money card 19A and terminal ID"T150" are registered into the invalid card ID list and the accident terminal ID list. When card ID"C99" and terminal ID"T150" which received were not registered into an invalid card ID list and an accident terminal ID list and they are distinguished, the electronic money server 13, A dealings attestation child {Pk1A (T150"+ transaction information +C99)} is changed into transaction information, card ID, and terminal ID using individual public key Pk2A which received. A customer attestation child {Tk1B (T150"+ transaction information +C99)} is changed into transaction information, card ID, and terminal ID using terminal public key Tk2B which received, and it is distinguished whether these are mutually in agreement. When in agreement, the electronic money server 13 transmits card ID"C99" and individual public key Pk2A to the certificate authority 11 with an attestation grant demand (L54).

[0179]If the certificate authority 11 confirms whether card ID"C99" and individual public key Pk2A which received are registered into the system with reference to card ID and the individual public key which self has memorized and a registered thing is checked, Certification information {Ck1 (C99+Pk2A)} is generated using center public key Ck1, and it transmits to the electronic money server 13 with the completion wording of a telegram of attestation (L55). The electronic money server 13 will distinguish whether the balance of card ID"C99" of a balance table is 50,000 yen or more of the amount of money for liquidation, if the completion wording of a telegram of attestation and certification

information {Ck1 (C99+Pk2A)} are received from the certificate authority 11. if the balance of 50,000 yen or more becomes -- the electronic money server 13 -- the bank center 17 -- card ID"C99" and transfer amount -- the change request wording of a telegram containing "50,000 yen" is transmitted (L56).

[0180]The bank center 17 will change 50,000 yen to the settlement account of the user A corresponding to card ID"C99" from an account specially with reference to an account table, if change request wording of a telegram is received from the electronic money server 13. If transfer processing is completed, the bank center 17 will transmit change completion wording of a telegram to the electronic money server 13 (L57). If change completion wording of a telegram is received, the electronic money server 13 will subtract 50,000 yen from the balance of card ID"C99" of a balance table, will generate a transaction history, and will memorize it on a transaction history table. Next, the electronic money server 13 gives the certification information {Ck1 (C99+Pk2A)} from the certificate authority 11 to a transaction history, and transmits to the electronic money terminal 15B with the completion wording of a telegram of liquidation (L58).

[0181]The electronic money terminal 15B answers the completion wording of a telegram of liquidation, using center public key Ck2, changes certification information {Ck1 (C99+Pk2A)} into the card C99 and individual public key Pk2, and checks it. If it checks that the certification information is a right thing, a transaction history will be transmitted to the electronic money card 19A (L59). IC part 20 of the electronic money card 19A subtracts 50,000 yen from the balance which self memorizes based on the received transaction history. The electronic money terminal 15B adds the received transaction history to the position which the last dealings pointer of the optical storing part 21 directs, and updates the value of the last dealings pointer and a transmitted pointer. Then, the electronic money terminal 15B displays on the indicator 32 that liquidation of electronic money was completed, and it discharges the electronic money card 19A.

[0182]Thus, the user can realize the electronic money accumulated in the self electronic money card 19, and can transfer a self settlement account.

[0183]As explained above, it can be used for charging electronic money to an electronic money card, converting into money, transferring, and paying with this electronic money system. And since a transaction history is recorded on the optical storing part 21, a malfeasance etc. are easily detectable by verifying the contents of record of this added type storage parts store of a postscript (tailing). A malfeasance can be more certainly detected by recording a transaction history also in a center.

[0184]This invention is not limited to the above-mentioned embodiment, but various modification and application are possible for it. For example, the component of a transaction history is arbitrary and may include dealings ID [meaning / each dealings], the balance of the electronic money in the time, a dealings time second, etc. in a transaction history. Certification information etc. may be deleted from a transaction history.

[0185]The information which specifies the card from the transaction history recorded on

the optical storing part 21 may be omitted. For example, when electronic money is charged to the electronic money card 19A, it is not necessary to record transaction money amount, terminal ID, etc. on the optical storing part 21 of the electronic money card 19A, and to record the information which specifies self on it at the time of that dealings are charge and a trade date, for example.

[0186]Similarly when electronic money is moved to the electronic money card 19B from the electronic money card 19A, for example to the optical storing part 21 of the electronic money card 19A. That dealings classification is transfer of electronic money, card ID of the electronic money card 19B of a transfer place, Record the amount of money for a transfer, etc., and do not record the information which specifies a transferring agency (electronic money card 19A), but to the optical storing part 21 of the electronic money card 19B. It may constitute so that card ID of the electronic money card 19A of being [it / the inheritance of electronic money] and transfer origin, the amount of money for a transfer, etc. may be recorded and the information which specifies a new address (electronic money card 19B) may not be recorded. Thereby, the quantity of the record data of the optical storing part 21 is reducible.

[0187]Although the list of settlement accounts of the user of an electronic money card was registered into the bank center 17 and card ID was changed into the account number of the settlement account in the above-mentioned embodiment, The account number of the settlement account is registered into IC part 20 or the optical storing part 21 of the electronic money card 19, and when processing charge of electronic money, liquidation, etc., an account number may be notified to the bank center 17 from the electronic money card 19.

[0188]In the above-mentioned embodiment, in order to generate and check personal authentication information, the signature key Sk and the check key Ek were used, but center secret key Ck1 and center public key Ck2 may be used.

[0189]When building this electronic money system on the networks (for example, Internet etc.) of the network of wide area, Although it is desirable to form the certificate authority 11 and the electronic money server 13, respectively, in a closed loop type local network, the certificate authority 11 and the electronic money server 13 may be realized as one server.

[0190]This electronic money system may be made the composition except the certificate authority 11 as shown in drawing 21. The outline of each processing in this case is shown in drawing 22 - drawing 26. The processing in this case is the same as operation of an embodiment, if **** whose processing about a center secret key and a center public key, an individual secret key and an individual public key, and attestation was lost is removed so that clearly, if a drawing drawing 22 - drawing 26, and old is referred to. According to this composition, processing speed improves in the whole system.

[0191]In order to raise the security of a system, the justification of the operator of the electronic money terminal 15 may be distinguished based on an operator's bodily features, for example. For example, only when the possessor's fingerprint data is arranged to the store circuit of IC part 20 of the electronic money card 19, the fingerprint of the operator of

the electronic money terminal 15 is scanned and these are in agreement, future electronic money transaction processings may be performed.

[0192]In this case, the fingerprint reader 41 as shown in drawing 27 is connected to the electronic money terminal 15. The fingerprint reader 41 is provided with the guide 41B for guiding the reading window 41A and finger for scanning a fingerprint. As shown in drawing 28, after carrying out the Fourier transform of the picture of a holder's fingerprint, the extracted topology is beforehand registered into the store circuit of IC part 20.

[0193]The image acquiring part 51 which the fingerprint reader 41 scans the picture (picture of a fingerprint) in the reading window 41A as shown in drawing 28, and acquires image data, The Fourier converter 52 which carries out the Fourier transform of the image data (waveform) acquired by the image acquiring part 51, The topology extraction part 53 which extracts only the topology of the Fourier series acquired by the Fourier converter 52, The phase composition part 54 which compounds the topology read from IC part 20, and the topology generated by the topology extraction part 53, It comprises a Fourier converter 55 which carries out the Fourier transform of the topology compounded by the synchronizer 54, and obtains correlation strength, and the discrimination section 56 which compares the correlation strength and the threshold which were acquired by the Fourier converter 55, and distinguishes whether an operator is a just person.

[0194]In such composition, if processing is chosen from processing menus and the electronic money card 19 is inserted, the electronic money terminal 15 will display the message of the purport that a finger is placed on the fingerprint reader 41, as shown in drawing 29. If an operator places a finger on the fingerprint reader 41 according to a message, the image acquiring part 51 of the fingerprint reader 41 will scan the fingerprint in the reading window 41A, and will capture the image. The Fourier converter 52 carries out the Fourier transform of the read picture, and the topology extraction part 53 incorporates topology.

[0195]Then, the phase composition part 54 reads the topology registered into IC part 20, and compounds with the topology extracted from the topology extraction part 53, and further, the Fourier converter 55 carries out the Fourier transform of the complex data, and asks for correlation strength.

[0196]The fingerprint beforehand registered into IC part 20 when correlation strength is beyond constant value, and the identified fingerprint are similar, and the judgment part 56 is controlled to enable processing after an operator distinguishes that he is a just holder of the electronic money card 19 and corresponds to the selected processing. Since it judges that the fingerprint beforehand registered into IC part 20 and the identified fingerprint are not similar and fingerprint authentication is not in agreement with the indicator 32 when correlation strength is less than constant value, it indicates that it cannot perform future operations and the electronic money card 19 is discharged.

[0197]According to such composition, based on an operator's bodily features, an operator can distinguish whether you are a just person and it can be distinguished whether dealings of electronic money are permitted. Therefore, the unauthorized use of electronic money can

be prevented effectively.

[0198]The technique and circuit which distinguish the similarity of a fingerprint are not limited to the circuit and method which are shown in drawing 28, but may use other techniques. As bodily features, not only a fingerprint but a voiceprint, the pattern of a face, retina patterns, etc. may be used. In using a voiceprint, it stores the characteristic data of a voiceprint in IC part 20, A microphone is arranged to the electronic money terminal 15, the characteristic data of the sound acquired with the microphone is extracted, and correlation strength with the characteristic data stored in IC part 20 is distinguished, and when correlation strength is beyond constant value, it distinguishes that an operator is a just person.

[0199]In using the pattern of a face, retina patterns, etc., The characteristic data of a picture which stored the characteristic data of a face and retina patterns in IC part 20, has arranged the camera to the electronic money terminal 15, and was acquired with the camera is extracted, and correlation strength with the characteristic data stored in IC part 20 is distinguished, and when correlation strength is beyond constant value, it distinguishes that an operator is a just person.

[0200]The characteristic data extracted beforehand may be stored in IC part 20, and may be stored in the optical storing part 21. The characteristic data in which the bodily features used on the occasion of dealings is shown may be recorded on the optical storing part 21 as a part of transaction history information.

[0201]The malfeasance which obtains information, including a user's card ID etc., becomes an owner of the card ID, clears up in the system handling electronic money, for example, and makes attestation profitably like can be considered. In order to prevent such a malfeasance, the security can be raised by using cipher systems, such as for example, a RSA method, and enciphering communication wording of a telegram etc.

[0202]In this case, for example, the certificate authority 11 generates and memorizes center secret key Ck1 and center public key Ck2. The certificate authority 11 shares center secret key Ck1 within the center 10 by copying center secret key Ck1 to the electronic money server 13. The certificate authority 11 distributes center public key Ck2 to each electronic money terminal 15 and electronic money card 19 grade beforehand via the electronic money server 13.

[0203]Each electronic money card 19 and the electronic money terminal 15 encipher each information, including a charge demand, various wording of a telegram, etc., using center public key Ck2, and transmit to the electronic money server 13. [Electronic money card 19 if it becomes card ID and an individual public key the electronic money terminal 15 if it becomes] The electronic money server 13 decrypts and processes those information using center secret key Ck1. The electronic money server 13 enciphers a transaction history using the individual public key sent from the electronic money card 19, and transmits to the electronic money card 19 via the electronic money terminal 15.

[0204]By using such a technique, the information from the electronic money card 19 and the electronic money terminal 15, Only the electronic money server 13 and the certificate

authority 11 in the center 10 can be decrypted, and without being referred to with the electronic money terminal 15, it is transmitted to the electronic money card 19, and the transaction history from the electronic money server 13 is decrypted. Security can be raised more by changing a secret key and a public key periodically.

[0205]The certificate authority 11 changes periodically or irregularly center secret key Ck1 and public key Ck2, and center public key Ck2 is transmitted to the electronic money terminal 15, and it transmits center secret key Ck1 to the electronic money server 13, respectively. When the electronic money card 19 is inserted in the electronic money terminal 15 after changing center secret key Ck1 and center public key Ck2, the electronic money terminal 15 notifies new center public key Ck2 to the electronic money card 19.

[0206]The method of encryption is not limited to a public key system, but a common key system may be used for it. In this case, it is desirable to strengthen the tamper-proof nature of the electronic money card 19 from the field of security.

[0207]The keys (a secret key, the pair of a public key, a common key, etc.) of encryption new whenever dealings are conducted by this system are published, it may notify to an electronic money card and encryption and decryption may be performed using the notified key.

[0208]A key may be generated based on a random number. According to such a system, prediction of the key published next does not stick but disclosure of information can be prevented. It may be used as a key for encryption and decryption combining the key published in the past and the newly published key. For example, a variety of information may be enciphered combining this key K_t and the last key K_{t-1}, using $\{K_t+K_{t-1}\}$ as a key, and it may decrypt further.

[0209]In an electronic money system, it is possible to create and use improperly the perfect copy of electronic money card 19 the very thing. In order to prevent this kind of unauthorized use, a peculiar number is given to the electronic money card 19 for every dealings by the electronic money server 13, At the time of an online trade start, this specific number is transmitted to the electronic money server 13 from the electronic money card 19, What is necessary is to trade, after checking that it is in agreement with the specific number of the electronic money card 19 registered into the electronic money server, and just to constitute at the time of a transaction end, etc., so that a new specific number may be generated and it may register with the electronic money card 19 and the electronic money server 13. Since a specific number differs from what is registered into the electronic money server 13, it becomes impossible to use it except one used sheet, if according to this composition dealings are conducted once even if it creates the copy of the electronic money card 19 since a specific number is updated by the degree of dealings. Therefore, the unauthorized use by the copy of the electronic money card 19 can be prevented.

[0210]Although the cash of the amount of charge money is moved to the settlement account of a system from a user's account and he is trying to pay this amount of charge money on the occasion of charge processing of the electronic money to a card in the above-mentioned explanation, it is good also as payment by a credit (credit accommodation), for example. In

this case, for example, the server carries out fixed time memory according to reception of a charge demand by making into loan information the information, including the account of the amount of charge money, and a user, etc., which this demand shows, and pulls down from a user's account to predetermined timing. The account only for credit accommodation is prepared and a server pulls out the amount of charge money which this demand shows from the account according to reception of a charge demand. It may be made like. In this case, if there is payment, the amount of money for payment will be transferred to that user's loan account. When publishing electronic money by the credit or loan, it is desirable to check that there are more the amount of credit accommodation, the balance (** frame) which can be loaned, etc. than the frame of which issue was required. In addition, the economic ground of issue of electronic money itself is arbitrary.

[0211]The electronic money terminal of this invention cannot be based on a system for exclusive use, but can be realized using the usual computer system. For example, the electronic money terminal which performs above-mentioned processing can be constituted by installing this program from the media (a floppy disk, CD-ROM, etc.) which stored the program for performing above-mentioned operation in the computer.

[0212]Communication media (medium which holds a program temporarily and fluidly like a communication line, a communication network, and a communications system) may be sufficient as the medium for supplying a program to a computer. For example, this program may be put up for the bulletin board (BBS) of a communication network, and this may be distributed via a network. And above-mentioned processing can be performed by starting this program and performing like other application programs under control of OS.

[0213]

[Effect of the Invention]As explained above, according to this invention, electronic money can be charged to an electronic money card, and various dealings can be conducted to it using the charged electronic money. And since a transaction history is recorded on the added type storage parts store of a postscript, when abnormalities occur, a malfeasance etc. can be easily detected by verifying the contents of record of this added type storage parts store of a postscript. A malfeasance can be more certainly detected by recording a transaction history also in a center. When trading in electronic money, the reliability of dealings can be improved by distinguishing the justification based on an operator's bodily features.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the composition of the electronic money system concerning an embodiment of the invention.

[Drawing 2]The figure showing the structure of an invalid card list where the electronic money server has memorized the figure showing the structure of a balance table where the electronic money server has memorized (A), and (B), and (C) are the figures showing the

structure of the accident terminal list which the electronic money server has memorized.
[Drawing 3]It is a figure showing the structure of the transaction history table which the electronic money server has memorized.
[Drawing 4](A) and (B) are the figures showing the example of the appearance composition of an electronic money terminal.
[Drawing 5]It is a figure showing the structure of the account table which the bank center has memorized.
[Drawing 6]It is a figure showing the structure of an electronic money card.
[Drawing 7]It is a figure showing the outline of electronic money charge processing.
[Drawing 8](A) - (C) is a figure showing the display example of an electronic money terminal.
[Drawing 9]It is a figure for explaining the flow of electronic money charge processing.
[Drawing 10]It is a figure showing the outline of personal authentication information issuing processing.
[Drawing 11]It is a figure for explaining the flow of personal authentication information issuing processing.
[Drawing 12]It is a figure showing the outline of electronic money payment processing.
[Drawing 13]It is a figure for explaining the flow of electronic money payment processing.
[Drawing 14]It is a figure showing the outline of comparison processing.
[Drawing 15]It is a figure for explaining the flow of comparison processing.
[Drawing 16]It is a figure showing the state of the IC part transmission before of a non-transmission history, and after transmission, an optical storing part, and a balance table in comparison processing.
[Drawing 17]It is a figure showing the outline of electronic money transfer processing.
[Drawing 18]It is a figure for explaining the flow of electronic money transfer processing.
[Drawing 19]It is a figure showing the outline of electronic money liquidation processing.
[Drawing 20]It is a figure for explaining the flow of electronic money liquidation processing.
[Drawing 21]It is a figure showing an example of the composition of an electronic money system in case a certificate authority is not included.
[Drawing 22]It is a figure showing the flow of electronic money charge processing in case a certificate authority is not included.
[Drawing 23]It is a figure showing the flow of electronic money payment processing in case a certificate authority is not included.
[Drawing 24]It is a figure showing the flow of comparison processing in case a certificate authority is not included.
[Drawing 25]It is a figure showing the flow of electronic money transfer processing in case a certificate authority is not included.
[Drawing 26]It is a figure showing the flow of electronic money liquidation processing in case a certificate authority is not included.
[Drawing 27]It is a figure showing the example of a fingerprint reader.
[Drawing 28]It is a figure showing the example of composition of a fingerprint

authentication circuit.

[Drawing 29]It is a figure showing the display example of the electronic money terminal at the time of fingerprint authentication.

[Description of Notations]

10 Center

11 Certificate authority

13 Electronic money server

15 Electronic money terminal

19 Electronic money card

20 IC part

21 Optical storing part

30 Storage parts store

31 Input part

32 Indicator

33 Card processing part

34 Touch panel

35, 35A, 35B card slot

36 Money drawer

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－154192

(43)公開日　平成10年(1998)６月９日

(51)Int.Cl.[6]	識別記号	FI	
G06F 19/00		G06F 15/30	350
G06K 17/00		G06K 17/00	L
			S
G07D 9/00	451	G07D 9/00	451C
	461		461A

審査請求　未請求　請求項の数33　ＯＬ　（全 32 頁）　最終頁に続く

(21)出願番号　特願平9－251907

(22)出願日　平成９年(1997)９月17日

(31)優先権主張番号　特願平8－255947

(32)優先日　平８(1996)９月27日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000102728
エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目３番３号

(72)発明者　古橋　信夫
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　部田　智
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　柴田　淳
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(74)代理人　弁理士　木村　満

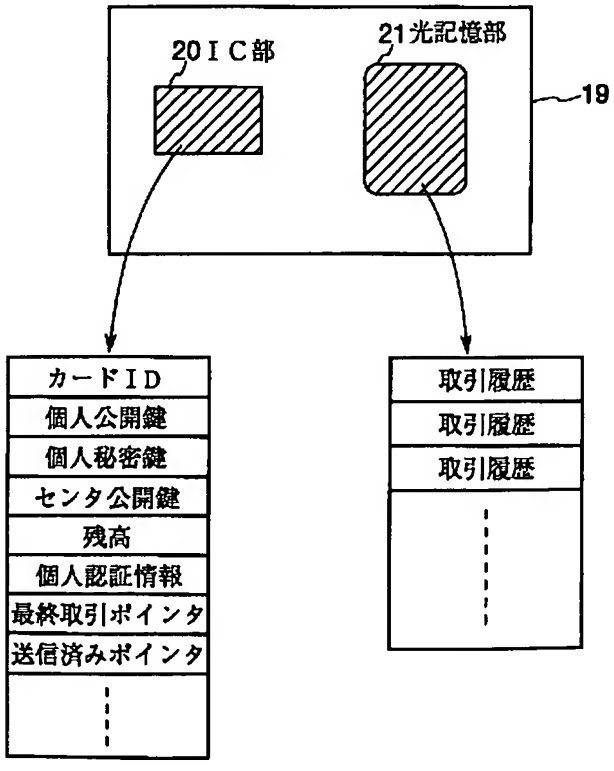
最終頁に続く

(54)【発明の名称】　電子マネーシステム及び記録媒体

(57)【要約】

【課題】　金銭データの偽造等を有効に防止し、且つ、不正な取引を容易に検出することを可能とする電子マネーシステムを提供することを目的とする。

【解決手段】　金銭的価値を有する電子マネーを格納する電子マネーカード１９を用いて電子マネーを取引する電子マネーシステムにおいて、電子マネーカード１９として、ＩＣ部２０と光記憶部２１とを備えるものを使用する。ＩＣ部２０には、電子マネーカード１９を特定するための情報、残高、光記憶部２１をアクセスするための情報等を記録し、光記憶部２１には、その電子マネーカードを用いて行われた電子マネーの取引の全ての履歴を記録する。電子マネー取引システムのコンピュータにも取引履歴を登録する。取引履歴を追跡することにより、不正の発生箇所、額等を検出できる。



1

【特許請求の範囲】

【請求項１】追記型記憶部とＩＣメモリ部とを備え、金銭的価値に関する情報を格納する電子マネーカードと、該電子マネーカードを処理する複数の端末と、該複数の端末と通信回線で接続されたコンピュータと、より構成される電子マネーシステムであって、

前記追記型記憶部は取引履歴情報を記憶し、

前記ＩＣメモリ部は、前記追記型記憶部に記憶された取引履歴情報の最終位置を示す位置情報を記憶し、

前記複数の端末は、金銭的価値に関する情報を前記電子マネーカードに記憶させることの指示と取引金額とを入力する入力手段と、前記入力手段により入力された指示及び取引金額と口座を特定するための口座特定情報とをチャージ要求電文として前記コンピュータに送信する指示電文送信手段と、を備え、

前記コンピュータは、前記チャージ要求電文を受信する手段と、受信した前記チャージ要求電文のなかの口座特定情報が特定する口座から取引金額が示す金額を所定口座に移動する金額移動手段と、前記金額移動手段による金額の移動が完了したことを示す応答電文を送信する応答電文送信手段と、を備え、

更に前記複数の端末は、前記応答電文の受信に応答し、前記ＩＣメモリ部に格納された位置情報に従って、前記応答電文に対応する取引履歴情報を前記追記型記憶部に書き込む手段を備える、

ことを特徴とする電子マネーシステム。

【請求項２】前記電子マネーカードの前記追記型記憶部は、光エネルギーが照射されることにより物理的にピットが形成されてデータが書き込まれ、書き換えが不可能な光記憶部から構成されている、ことを特徴とする請求項１に記載の電子マネーシステム。

【請求項３】前記電子マネーカードの前記追記型記憶部と前記ＩＣメモリ部の少なくとも一方は、前記口座特定情報を記憶しており、

前記指示電文送信手段は、前記電子マネーカードに記憶された前記口座特定情報を読み出す手段と、読み出された口座特定情報を送信する手段と、より構成されている、ことを特徴とする請求項１又は２に記載の電子マネーシステム。

【請求項４】前記コンピュータは、前記口座特定情報により特定される口座の残高が前記チャージ要求電文により指示される取引金額以上か否かを判別し、残高が該取引金額未満ならば、エラーメッセージを前記端末に送信すると共に取引を中止する手段を備える、

ことを特徴とする請求項１、２又は３に記載の電子マネーシステム。

【請求項５】前記取引履歴情報は、各取引について、取引の種別と、取引年月日と、その取引を処理した前記端末を特定する情報と、取引金額とを含む、ことを特徴とする請求項１乃至４のいずれか１項に記載の電子マネーシステム。

2

【請求項６】前記電子マネーカードの前記追記型記憶部は、該電子マネーカードで取引された全ての取引の取引履歴を記憶する、ことを特徴とする請求項１乃至５のいずれか１項に記載の電子マネーシステム。

【請求項７】前記コンピュータは、前記電子マネーカードの電子マネーの全ての取引の取引履歴を記憶する取引履歴記憶手段を備える、ことを特徴とする請求項１乃至６のいずれか１項に記載の電子マネーシステム。

【請求項８】前記電子マネーカードの前記追記型記憶部と前記ＩＣメモリ部との少なくとも一方はその電子マネーカードのカード識別符号を記憶し、

前記チャージ要求電文は前記カード識別符号を含み、

前記コンピュータは、使用を認めない前記電子マネーカードの前記カード識別符号を不正カードＩＤとして記憶する不正カードＩＤ記憶手段と、前記チャージ要求電文に含まれる前記カード識別符号と前記不正カードＩＤ記憶手段に記憶されている前記不正カードＩＤとを比較し、一致する不正カードＩＤを検出すると、取引を中止する手段を備える、ことを特徴とする請求項１乃至７のいずれか１項に記載の電子マネーシステム。

【請求項９】各前記端末は端末識別符号を記憶し、

前記チャージ要求電文は前記端末識別符号を含み、

前記コンピュータは、使用を認めない前記端末の前記端末識別符号を不正端末ＩＤとして記憶する不正端末ＩＤ記憶手段と、前記チャージ要求電文に含まれる前記端末識別符号を前記不正端末ＩＤ記憶手段に記憶される前記不正端末ＩＤと比較し、一致する不正端末ＩＤを検出すると、取引を中止する手段を備える、ことを特徴とする請求項１乃至８のいずれか１項に記載の電子マネーシステム。

【請求項１０】前記ＩＣメモリ部は一対の個人公開鍵と個人秘密鍵を記憶し、

前記電子マネーカードの前記個人公開鍵を複数記憶する個人情報記憶手段を備える認証局を更に備え、

前記チャージ要求電文は、前記電子マネーカードの前記個人公開鍵を含み、

前記コンピュータは、受信したチャージ要求電文のうち、前記個人公開鍵を前記認証局に送信する個人鍵送信手段を備え、

前記認証局は、受信した前記個人公開鍵を前記個人情報記憶手段に記憶されている複数の個人公開鍵のいずれかと一致するか否かを判別し、一致しない場合、取引不可の旨のメッセージを前記端末に送信することにより取引を中止する手段を更に備える、

ことを特徴とする請求項１乃至９のいずれか１項に記載の電子マネーシステム。

【請求項１１】前記追記型記憶部又は前記ＩＣメモリ部はカード識別符号を記憶し、

前記電子マネーカードの前記カード識別符号を複数記憶

する個人情報記憶手段を備える認証局を更に備え、
前記チャージ要求電文は、前記カード識別符号を含み、
前記コンピュータは、受信したカード識別符号を前記認証局に送信する手段を備え、
前記認証局は、受信した前記カード識別符号を前記個人情報記憶手段に記憶されている複数のカード識別符号のいずれかと一致するか否かを判別し、一致しない場合、取引不可の旨のメッセージを前記端末に送信して取引を中止する手段を更に備える、
ことを特徴とする請求項１乃至９のいずれか１項に記載の電子マネーシステム。
【請求項１２】各前記ＩＣメモリ部は、一対の個人公開鍵と個人秘密鍵を備え、
各前記端末は、一対の端末公開鍵と端末秘密鍵を備え、
前記チャージ要求電文は、取引に関する情報と前記個人秘密鍵を用いて前記電子マネーカードにより生成された第１の認証子と、前記取引に関する情報と前記端末秘密鍵を用いて前記端末により生成された第２の認証子と前記個人公開鍵と前記端末公開鍵とを含み、
前記コンピュータは、前記個人公開鍵と前記端末公開鍵とを用いて前記第１と第２の認証子が一致するか否かを判別し、一致する場合にのみ、前記チャージを行うための処理を実行する、
ことを特徴とする請求項１乃至１１のいずれか１項に記載の電子マネーシステム。
【請求項１３】前記電子マネーカードの追記型記憶部に記憶される取引履歴は該電子マネーカードを特定する情報を含まない、ことを特徴とする請求項１乃至１２のいずれか１項に記載の電子マネーシステム。
【請求項１４】前記電子マネーカードの前記ＩＣメモリ部と前記追記型記憶部の一方は、使用者の身体的特徴を示す特徴データを記憶しており、
前記複数の端末は、操作者の身体的特徴を示す特徴データを取得する取得手段と、前記電子マネーカードから特徴データを読み込む読込手段と、前記取得手段により取得された特徴データと前記読込手段により読み込まれた特徴データとを比較し、実質的に一致するか否かを判別する判別手段と、前記判別手段が実質的に一致すると判断した時に、該端末を介した電子マネーの取引を可能とし、前記判別手段が実質的に一致しないと判断した時に、該端末を介した電子マネーの取引を禁止する取引制御手段と、を備える、
ことを特徴とする請求項１乃至１３のいずれか１項に記載の電子マネーシステム。
【請求項１５】金銭的価値を有する電子的情報である電子マネーを取引するための電子マネーシステムであって、
少なくとも残高を含む前記電子マネーに関する情報と自己を特定するためのカード識別符号とを記憶する第１の記憶手段と、前記電子マネーの取引履歴を記憶する第２の記憶手段と、を備える複数の電子マネーカードと、
各前記電子マネーカードに対応する決済口座を備える銀行センタと、
自己を特定するための端末識別符号が付されており、前記電子マネーカードが装着され、所定金額の前記電子マネーを装着された電子マネーカードに補充するよう指示するチャージ要求を入力するためのチャージ要求入力手段と、前記チャージ要求を送信するチャージ要求送信手段と、を備える電子マネー取引装置と、
前記複数の電子マネーカードの残高を記憶する残高記憶手段と、前記電子マネー取引装置からの前記チャージ要求に従って、該電子マネーカードに対応する前記決済口座から他の所定口座へ前記所定金額を移動するよう前記銀行センタに指示するチャージ指示手段と、前記残高記憶手段に記憶されている該電子マネーカードの残高に前記所定金額を加算する手段と、取引履歴を記憶する取引履歴記憶手段と、取引の完了を示す取引完了通知を前記電子マネー取引装置に送信する取引完了通知送信手段と、を備えるコンピュータと、
前記電子マネー取引装置は、前記取引完了通知送信手段からの前記取引完了通知に応答して、取引履歴を前記第２の記憶手段に書き込む履歴書き込み手段と、前記第１の記憶手段に記憶されている残高に前記チャージ要求が指示する前記所定金額を加算するカード残高更新手段と、を更に備える、
ことを特徴とする電子マネーシステム。
【請求項１６】前記コンピュータは、該電子マネーカードに対応する前記決済口座の残高が前記チャージ要求により指示される前記所定金額以上か否かを判別し、該残高が該所定金額未満ならば、エラーメッセージを前記電子マネー取引装置に送信する手段と、取引を中止する手段と、を備える、
ことを特徴とする請求項１５に記載の電子マネーシステム。
【請求項１７】前記電子マネーカードにおいて、前記第１の記憶手段は、メモリを備えるＩＣチップにより構成され、前記第２の記憶手段は、書き換え不可能な記憶媒体により構成される、ことを特徴とする請求項１５又は１６に記載の電子マネーシステム。
【請求項１８】前記取引履歴は、前記電子マネーカードの前記カード識別符号と前記電子マネー取引装置の前記端末識別符号とを含む、ことを特徴とする請求項１５、１６又は１７に記載の電子マネーシステム。
【請求項１９】前記電子マネーカードに記録される取引履歴は、該電子マネーカード自身を特定するための情報を含まない、ことを特徴とする請求項１５、１６、１７又は１８に記載の電子マネーシステム。
【請求項２０】前記取引履歴は、取引年月日と、前記チャージ要求を送信した前記電子マネー取引装置の前記端末識別符号と、取引金額とを含む、ことを特徴とする請

求項１５、１６又は１７に記載の電子マネーシステム。

【請求項２１】前記電子マネーカードの前記第２の記憶手段は、該電子マネーカードで取引された全ての取引の取引履歴を記憶する、ことを特徴とする請求項１５乃至２０のいずれか１項に記載の電子マネーシステム。

【請求項２２】前記コンピュータの前記取引履歴記憶手段は、前記電子マネーカードで取引された全ての取引の取引履歴を記憶する、ことを特徴とする請求項１５乃至２１のいずれか１項に記載の電子マネーシステム。

【請求項２３】前記電子マネー取引装置の前記チャージ要求送信手段により送信されるチャージ要求は、該電子マネー取引装置に挿入されている電子マネーカードの前記カード識別符号を含み、

前記コンピュータは、使用を認めない前記電子マネーカードの前記カード識別符号を不正カードＩＤとして記憶する不正カードＩＤ記憶手段と、前記チャージ要求に含まれる前記カード識別符号を前記不正カードＩＤ記憶手段に記憶されている前記不正カードＩＤと比較し、一致するか否かを判別する手段と、を備えることにより不正な電子マネーカードを検出することができることを特徴とする請求項１５乃至２２のいずれか１項に記載の電子マネーシステム。

【請求項２４】前記電子マネー取引装置の前記チャージ要求送信手段により送信されるチャージ要求は、該電子マネー取引装置の前記端末識別符号を含み、

前記コンピュータは、使用を認めない前記電子マネー取引装置の前記端末識別符号を不正端末ＩＤとして記憶する不正端末ＩＤ記憶手段と、前記チャージ要求に含まれる前記端末識別符号を前記不正端末ＩＤ記憶手段に記憶される前記不正端末ＩＤと比較し、一致するか否かを判別する手段と、を備えることにより不正な電子マネー取引装置を検出することができることを特徴とする請求項１５乃至２３のいずれか１項に記載の電子マネーシステム。

【請求項２５】この電子マネーシステムに登録されている電子マネーカードの登録リストを記憶する認証局を更に備え、

前記チャージ要求は、前記電子マネーカードを特定するための特定データを含み、

前記認証局は、前記チャージ要求に含まれている特定データが、登録リストに登録されているか否かを判別し、登録されていない場合、取引を中止する手段を備える、ことを特徴とする請求項１５乃至２４のいずれか１項に記載の電子マネーシステム。

【請求項２６】前記電子マネーカードは、一対の個人公開鍵と個人秘密鍵を備え、

前記電子マネー取引装置は、一対の端末公開鍵と端末秘密鍵を備え、

前記チャージ要求は、取引に関する情報と前記個人秘密鍵を用いて生成された第１の認証子と、前記取引に関する情報と前記端末秘密鍵を用いて生成された第２の認証子と前記個人公開鍵と前記端末公開鍵とを含み、

前記コンピュータは、前記個人秘密鍵と前記端末秘密鍵とを用いて前記第１と第２の認証子が一致するか否かを判別する、

ことを特徴とする請求項１５乃至２５のいずれか１項に記載の電子マネーシステム。

【請求項２７】前記電子マネーカードの前記第１の記憶手段と前記第２の記憶手段の一方は使用者の身体的特徴を示す特徴データを記憶しており、

前記電子マネー取引装置は、操作者の身体的特徴を示す特徴データを取得する取得手段と、前記電子マネーカードから特徴データを読み込む読込手段と、前記取得手段により取得された特徴データと前記読込手段により読み込まれた特徴データとを比較し、実質的に一致するか否かを判別する判別手段と、前記判別手段が実質的に一致すると判断した時に、該電子マネー取引装置を介した電子マネーの取引を可能とし、前記判別手段が実質的に一致しないと判断した時に、該電子マネー取引装置を介した電子マネーの取引を禁止する取引制御手段と、を備える、

ことを特徴とする請求項１５乃至２６のいずれか１項に記載の電子マネーシステム。

【請求項２８】金銭的価値を有する電子マネーを格納する電子マネーカードを用いて電子マネーを取引する電子マネーシステムにおいて、

前記電子マネーカードは、追記型記憶部とＩＣメモリ部とを備え、

前記ＩＣメモリ部は、その電子マネーカードを特定するための情報及び前記追記型記憶部をアクセスするための情報を記憶し、

前記電子マネーシステムは、前記電子マネーカードに格納されている電子マネーを取引する取引手段と、前記電子マネーカードの前記追記型記憶部に、該電子マネーカードを用いて行われた電子マネーの取引の履歴を記憶する履歴記録手段とを備える、

ことを特徴とする電子マネーシステム。

【請求項２９】前記電子マネーシステムは、さらに、この電子マネーシステムで行われた電子マネーの取引の履歴を記憶する履歴記憶手段を備える、

ことを特徴とする請求項２８に記載の電子マネーシステム。

【請求項３０】電子マネー情報が記録されている媒体を用いて電子マネーを取引する電子マネーシステムにおいて、

媒体に記録されている利用者の身体的特徴に関する特徴データを読み取る読取手段と、

カード利用者の身体の全体もしくは一部をスキャンするスキャン手段と、

前記スキャン手段によりスキャンしたデータを媒体に記

録されているデータの形式に変換する手段と、
変換後のデータと前記媒体に記録されているデータを比較する手段と、
前記データの比較で一致度を判定する手段と、
上記判定結果が一定値以上の場合、電子マネー取引を有効とする手段と、
を有することを特徴とする電子マネーシステム。

【請求項３１】コンピュータを、追記型記憶部とＩＣメモリ部とを備えており金銭的価値に関する情報を格納する電子マネーカードを処理する複数の端末と、該複数の端末と通信により接続されたセンタと、を備えるシステムにおける前記端末として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、
該コンピュータを、金銭的価値に関する情報を前記電子マネーカードに記憶させることの指示と取引金額とを入力する入力手段、前記入力手段により入力された指示及び取引金額と、口座を特定するための口座特定情報と、をチャージ要求電文として前記センタに送信する送信手段、前記チャージ要求電文に応答して前記センタから返送されてきたチャージ許可電文を受信し、前記電子マネーカードの前記ＩＣメモリ部から、データを書き込むべき位置を示す位置情報を読み出し、該位置情報に従って、前記金銭的価値に関する情報を含む取引履歴情報を前記電子マネーカードの前記追記型記憶部に書き込む手段、として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項３２】コンピュータを、金銭的価値を有する電子的情報である電子マネーを取引するための電子マネーシステムにおける電子マネー情報とカード識別符号と電子マネーの取引履歴とを記憶する電子マネーカードを処理する電子マネー取引装置として機能させるコンピュータ読み取り可能記録媒体であって、
該コンピュータを、所定金額相当の電子マネーの前記電子マネーカードへの補充を要求するチャージ要求を入力するチャージ要求入力手段、前記チャージ要求をセンタに送信するチャージ要求送信手段、前記チャージ要求に応答して返送される前記センタからの通知に応答して、取引履歴を前記電子マネーカードに記録するとともに、該電子マネーカードに記憶されている残高に前記所定金額を加算するカード更新手段、として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項３３】コンピュータを、カード利用者の身体の全体もしくは一部をスキャンするスキャン手段、前記スキャン手段によりスキャンしたデータを所定形式に変換する変換手段、電子マネー情報が記録されている媒体に記録されている利用者の身体的特徴に関する特徴データを読み取る読取手段、前記読取手段により読み取られたデータと前記変換手段により変換されたデータとを比較する手段、前記データの比較における一致度を判定する手段、上記判定結果が一定値以上の場合、電子マネー取引を有効とする手段、として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、金銭的情報である電子マネーを取引する電子マネーシステムに関する。

【０００２】

【従来の技術】貨幣的価値を有する金銭データを用いて電子的な決済を可能とする電子マネーシステムが例えば、特公平７－１１１７２３等に開示されている。

【０００３】

【発明が解決しようとする課題】電子マネーシステムでは、権限を有していない者の使用、金銭データのコピー、偽造等を有効に防止する必要がある。また、偽造等された金銭データの使用を発見した場合には、その流通経路を追跡し、不正元・偽造元等を発見できることが望ましい。しかし、このような要請を満たす電子マネーシステムは、未だに、提案されていない。

【０００４】本発明は、上記実状に鑑みてなされたもので、金銭データの偽造等を有効に防止することができる電子マネーシステムを提供することを目的とする。また、本発明は、不正な取引を容易に検出し、その追跡性に優れた電子マネーシステムを提供することを目的とする。

【０００５】

【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点に係る電子マネーシステムは、追記型記憶部とＩＣメモリ部とを備え、金銭的価値に関する情報を格納する電子マネーカードと、該電子マネーカードを処理する複数の端末と、該複数の端末と通信回線で接続されたコンピュータと、より構成される電子マネーシステムであって、前記追記型記憶部は、取引を特定するための取引特定符号と、取引金額と残高の少なくとも一方と、を含む取引履歴情報を記憶し、前記ＩＣメモリ部は、前記追記型記憶部に記憶された取引履歴情報の最終位置を示す位置情報を記憶し、前記複数の端末は、金銭的価値に関する情報を前記電子マネーカードに記憶させることの指示と取引金額とを入力する入力手段と、前記入力手段により入力された指示及び取引金額と口座を特定するための口座特定情報とをチャージ要求電文として前記コンピュータに送信する指示電文送信手段と、を備え、前記コンピュータは、前記チャージ要求電文を受信する手段と、受信した前記チャージ要求電文のなかの口座特定情報が特定する口座から取引金額が示す金額を所定口座に移動する金額移動手段と、前記金額移動手段による金額の移動が完了したことを示す応答電文を送信する応答電文送信手段と、を備え、更に前記複数の端末は、前記応答電文の受信に応答し、前記ＩＣメ

モリ部に格納された位置情報に従って、前記応答電文に対応する取引履歴情報を前記追記型記憶部に書き込む手段を備える、ことを特徴とする。

【０００６】このような構成によれば、電子マネーカードに電子マネーをチャージし、チャージした電子マネーを用いて種々の取引を行うことができる。しかも、追記型記憶部に取引履歴を記録するので、異常が発生した場合に、この追記型記憶部の記録内容を検証することにより、不正行為等を容易に検出することができる。なお、電子マネーカードは、実体として電子マネーカードの機能を有していればよく、その形状は、箱、円盤、ノート、手帳等、任意である。また、口座は、普通預金口座、当座預金口座、貸付口座等任意であり、電子マネーを発生する経済的根拠（現金であるか、貸し付けであるか等）は任意である。

【０００７】前記追記型記憶部は、例えば、光エネルギーが照射されることにより物理的にピットが形成されてデータが書き込まれ、書き換えが不可能な光記憶部から構成される。

【０００８】前記電子マネーカードの前記追記型記憶部と前記ＩＣメモリ部の少なくとも一方は、前記口座特定情報を記憶しており、前記指示電文送信手段は、前記電子マネーカードに記憶された前記口座特定情報を読み出す手段と、読み出された口座特定情報を送信する手段と、より構成されている。口座特定情報としては、口座番号自体でもよく、或いは、口座番号と対応する他の番号、例えばカードＩＤ等でもよい。

【０００９】前記コンピュータは、前記口座特定情報により特定される口座の残高が前記チャージ要求電文により指示される取引金額以上か否かを判別し、残高が該取引金額未満ならば、エラーメッセージを前記端末に送信すると共に取引を中止する手段を備えてもよい。このような構成とすることにより、取引の安全性を高めることができる。

【００１０】前記取引履歴情報は、各取引について、取引の種別、取引年月日と、その取引を処理した前記端末を特定する情報と、取引金額とを含む。これらの情報を追跡することにより、不正箇所等を判別することができる。この場合、前記電子マネーカードの前記追記型記憶部に、該電子マネーカードで取引された全ての取引の取引履歴を記憶させることが望ましい。

【００１１】前記コンピュータは、前記電子マネーカードで取引された全ての取引の取引履歴を記憶する取引履歴記憶手段を備えてもよい。電子マネーカードに登録された取引履歴とコンピュータに記録された取引履歴を突き合わせることにより、より容易に不正等を検出することができる。

【００１２】前記チャージ要求電文に電子マネーカードを特定するためのカード識別符号を含ませ、前記コンピュータには、使用を認めない前記電子マネーカードの前記カード識別符号を不正カードＩＤとして記憶する不正カードＩＤ記憶手段と、前記チャージ要求電文に含まれる前記カード識別符号と前記不正カードＩＤ記憶手段に記憶されている前記不正カードＩＤとを比較し、一致する不正カードＩＤを検出すると、取引を中止する手段を配置してもよい。このような構成によれば、登録された事故カード等が使用された場合、それを検出し、取引を中止できる。

【００１３】前記チャージ要求電文に前記端末識別符号を含ませ、前記コンピュータに、使用を認めない前記端末の前記端末識別符号を不正端末ＩＤとして記憶する不正端末ＩＤ記憶手段と、前記チャージ要求電文に含まれる前記端末識別符号を前記不正端末ＩＤ記憶手段に記憶される前記不正端末ＩＤと比較し、一致する不正端末ＩＤを検出すると、取引を中止する手段を配置してもよい。このような構成によれば、登録された事故端末等が使用された場合、それを検出し、取引を中止できる。

【００１４】各電子マネーカードに付された個人公開鍵及び／又はカード識別符号を付与し、これら個人公開鍵及び／又はカード識別符号がシステムに登録されているか否かを判別する認証局を配置してもよい。

【００１５】各ＩＣメモリ部は、一対の個人公開鍵と個人秘密鍵を備え、各前記端末は、一対の端末公開鍵と端末秘密鍵を備え、前記チャージ要求電文は、取引に関する情報と前記個人秘密鍵を用いて前記電子マネーカードにより生成された第１の認証子と、前記取引に関する情報と前記端末秘密鍵を用いて前記端末により生成された第２の認証子と前記個人公開鍵と前記端末公開鍵とを含み、前記コンピュータは、前記個人公開鍵と前記端末公開鍵とを用いて前記第１と第２の認証子が一致するか否かを判別し、一致する場合にのみ、前記チャージを行うための処理を実行する、ように構成してもよい。このような構成によれば、電子マネーカードの不正使用をより正確に検出することができる。

【００１６】前記電子マネーカードの追記型記憶部に記憶される取引履歴は該電子マネーカードを特定する情報を含まないようにしてもよい。このような構成によれば、追記型記憶部の容量を有効に使用することができる。

【００１７】操作者がこの電子マネーシステムを使用する権限を有しているか否かを、操作者の身体的特徴に基づいて判断してもよい。

【００１８】また、この発明の第２の観点にかかる電子マネーシステムは、金銭的価値を有する電子的情報である電子マネーを取引するための電子マネーシステムであって、少なくとも残高を含む前記電子マネーに関する情報と自己を特定するためのカード識別符号とを記憶する第１の記憶手段と、前記電子マネーの取引履歴を記憶する第２の記憶手段と、を備える複数の電子マネーカードと、各前記電子マネーカードに対応する決済口座を備え

る銀行センタと、自己を特定するための端末識別符号が付されており、前記電子マネーカードが装着され、所定金額の前記電子マネーを自己に補充するよう指示するチャージ要求を入力するためのチャージ要求入力手段と、前記チャージ要求を送信するチャージ要求送信手段と、を備える電子マネー取引装置と、前記複数の電子マネーカードの残高を記憶する残高記憶手段と、前記電子マネー取引装置からの前記チャージ要求に従って、該電子マネーカードに対応する前記決済口座から他の所定口座へ前記所定金額を移動するよう前記銀行センタに指示するチャージ指示手段と、前記残高記憶手段に記憶されている該電子マネーカードの残高に前記所定金額を加算する手段と、取引履歴を記憶する取引履歴記憶手段と、取引の完了を示す取引完了通知を前記電子マネー取引装置に送信する取引完了通知送信手段と、を備えるコンピュータと、前記電子マネー取引装置は、前記取引完了通知送信手段からの前記取引完了通知に応答して、取引履歴を前記第２の記憶手段に書き込む履歴書き込み手段と、前記第１の記憶手段に記憶されている残高に前記チャージ要求が指示する前記所定金額を加算するカード残高更新手段と、を更に備える、ことを特徴とする。

【００１９】このような構成によれば、電子マネーカードに電子マネーをチャージし、チャージした電子マネーを用いて種々の取引を行うことができる。しかも、追記型記憶部に取引履歴を記録するので、異常が発生した場合に、この追記型記憶部の記録内容を検証することにより、不正行為等を容易に検出することができる。決済口座は、普通預金口座、当座預金口座、貸付口座、クレジット口座など任意であり、電子マネーを発生する経済的根拠（対応金額の口座からの引き落としであるか、貸し付けであるか等）は任意である。

【００２０】前記コンピュータは、該電子マネーカードに対応する前記決済口座の残高（又は貸し付け限度額）が前記チャージ要求により指示される前記所定金額以上か否かを判別し、該残高が該所定金額未満ならば、エラーメッセージを前記電子マネー取引装置に送信する手段と、取引を中止する手段と、を備えてもよい。このような構成とすることにより、取引の安全性を高めることができる。

【００２１】例えば、前記電子マネーカードの前記第１の記憶手段は、メモリを備えるＩＣチップにより構成され、前記第２の記憶手段は、書き換え不可能な記憶媒体により構成される、ことを特徴とする。

【００２２】前記取引履歴は、前記電子マネーカードの前記カード識別符号と前記電子マネー取引装置の前記端末識別符号を含んでもよい。この構成によれば、不正行為等が行われたカードや端末を特定することができる。また、前記電子マネーカードに記録される取引履歴から、該電子マネーカードを特定するための情報を除去してもよい。各電子マネーカードに登録される取引履歴は、必ず、その電子マネーカードを使用している。従って、このデータを除去しても問題ない。

【００２３】前記取引履歴は、例えば、取引年月日と、前記チャージ要求を送信した前記電子マネー取引装置の前記端末識別符号と、取引金額とを含む。これらの情報を用いて取引を追尾することができる。

【００２４】前記電子マネーカードの前記第２の記憶手段は、例えば、該電子マネーカードで取引された全ての取引の取引履歴を記憶する。前記コンピュータの前記取引履歴記憶手段は、例えば、前記電子マネーカードで取引された全ての取引の取引履歴を記録する。このような構成とすることにより、取引を正確に追尾することができる。また、電子マネーカードに格納された取引履歴とコンピュータに格納された取引履歴を突き合わせることにより、不正の発生箇所等を容易に判別することができる。

【００２５】コンピュータに、使用が許可されていない、事故カード、事故端末等を登録しておき、これらのカード又は端末が使用された場合に、取引を禁止するようにしてもよい。

【００２６】電子マネーカードがこの電子マネーシステムで使用可能なものとして登録されているか否かを判別するための認証局を配置してもよい。この認証局は、例えば、電子マネーカードの個人公開鍵やカード識別符号が予め登録されているか否かを判別する。

【００２７】前記電子マネーカードは、一対の個人公開鍵と個人秘密鍵を備え、前記電子マネー取引装置は、一対の端末公開鍵と端末秘密鍵を備え、前記チャージ要求は、取引に関する情報と前記個人秘密鍵を用いて生成された第１の認証子と、前記取引に関する情報と前記端末秘密鍵を用いて生成された第２の認証子と前記個人公開鍵と前記端末公開鍵とを含み、前記コンピュータは、前記個人秘密鍵と前記端末秘密鍵とを用いて前記第１と第２の認証子が一致するか否かを判別する、ように構成してもよい。電子マネーカードと電子マネー取引装置の一方で不正が行われると第１の認証子と第２の認証子が一致しなくなる。従って、不正を判別することができる。

【００２８】なお、操作者の身体的特徴を示す特徴データを読み取り、これに基づいて、正当権限を有するものであるか否かを判別することができる。

【００２９】また、この発明の第３の観点にかかる電子マネーシステムは、金銭的価値を有する電子マネーを格納する電子マネーカードを用いて電子マネーを取引する電子マネーシステムにおいて、前記電子マネーカードは、追記型記憶部とＩＣメモリ部とを備え、ＩＣメモリ部は、電子マネーカードを特定するための情報及び前記追記型記憶部をアクセスするための情報を記憶し、前記電子マネーシステムは、前記電子マネーカードに格納されている電子マネーを取引する取引手段と、前記電子マネーカードの追記型記憶部に、該電子マネーカードを用

いて行われた電子マネーの取引の履歴を記憶する履歴記録手段とを備える、ことを特徴とする。このような構成によれば、各電子マネーカードでなされた電子マネーの取引を追記型記憶部に記録する。追記型記憶部の改竄は困難である。従って、追記型記憶部に記録された取引履歴を追尾することにより不正の有無等を判別することができる。

【００３０】前記電子マネーシステムは、さらに、この電子マネーシステムで行われた電子マネーの取引の履歴を記憶する履歴記憶手段を備えてもよい。このような構成とすることにより、より正確且つ容易に不正等を追尾することができる。

【００３１】また、この発明の第４の観点にかかる電子マネーシステムは、電子マネー情報が記録されている媒体を用いて電子マネーを取引する電子マネーシステムにおいて、媒体に記録されている利用者の身体的特徴に関する特徴データを読み取る読取手段と、カード利用者の身体の全体もしくは一部をスキャンするスキャン手段と、前記スキャン手段によりスキャンしたデータを前記媒体に記録されているデータの形式に変換する手段と、変換後のデータと媒体に記録されているデータを比較するスキャン手段と、前記データの比較で一致度を判定する手段と、上記判定結果が一定値以上の場合、電子マネー取引を有効とする手段と、を有することを特徴とする。このような構成によれば、操作者の正当性を操作者の身体的特徴に基づいて判別して、不正使用を有効に防止できる。

【００３２】なお、電子マネーシステムを、金銭的価値に関する情報を格納する電子マネーカードと、該電子マネーカードを処理する複数の端末と、該複数の端末と通信回線で接続されたコンピュータと、より構成される電子マネーシステムであって、前記複数の端末は、金銭的価値に関する情報を前記電子マネーカードに記憶させることの指示と取引金額とを入力する入力手段と、前記入力手段により入力された指示及び取引金額と口座を特定するための口座特定情報とをチャージ要求電文として前記コンピュータに送信するチャージ要求手段と、を備え、前記コンピュータは、前記チャージ要求電文を受信する手段と、受信した前記チャージ要求電文が示す口座特定情報と取引金額とを貸付情報として記憶し、チャージ応答電文を返送する手段と、更に前記複数の端末は、前記コンピュータからの前記チャージ応答電文の受信に応じて、金銭的価値に関する情報を含む取引履歴情報を前記プリペイドカードに記録する手段を備えるように構成してもよい。このような構成によれば、電子マネーカードに電子マネーをチャージし、チャージした電子マネーを用いて種々の取引を行うことができる。

【００３３】前記コンピュータは、前記貸付情報に基づいて、前記口座特定情報が特定する口座から前記取引金額を所定口座に移動する金額移動手段をさらに備えてもよい。

【００３４】また、この発明の第６の観点にかかる媒体は、コンピュータを、追記型記憶部とＩＣメモリ部とを備えており金銭的価値に関する情報を格納する電子マネーカードを処理する複数の端末と、該複数の端末と通信により接続されたセンタと、を備えるシステムにおける前記端末として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、該コンピュータを、金銭的価値に関する情報を前記電子マネーカードに記憶させることの指示と取引金額とを入力する入力手段、前記入力手段により入力された指示及び取引金額と、口座を特定するための口座特定情報と、をチャージ要求電文として前記センタに送信する送信手段、前記チャージ要求電文に応答して前記センタから返送されてきたチャージ許可電文を受信し、前記電子マネーカードの前記ＩＣメモリ部から、データを書き込むべき位置を示す位置情報を読み出し、該位置情報に従って、前記金銭的価値に関する情報を含む取引履歴情報を前記電子マネーカードの前記追記型記憶部に書き込む手段、として機能させるためのプログラムを記録する。このような構成によれば、電子マネーカードに電子マネーをチャージするための端末を通常のコンピュータを用いて実現することができる。

【００３５】また、この発明の第７の観点にかかる媒体は、コンピュータを、金銭的価値を有する電子的情報である電子マネーを取引するための電子マネーシステムにおける電子マネー情報とカード識別符号と電子マネーの取引履歴とを記憶する電子マネーカードを処理する電子マネー取引装置として機能させるコンピュータ読み取り可能記録媒体であって、該コンピュータを、所定金額相当の電子マネーの前記電子マネーカードへの補充を要求するチャージ要求を入力するチャージ要求入力手段、前記チャージ要求をセンタに送信するチャージ要求送信手段、前記チャージ要求に応答して返送される前記センタからの通知に応答して、取引履歴を前記電子マネーカードに記録するとともに、該電子マネーカードに記憶されている残高に前記所定金額を加算するカード更新手段、として機能させるためのプログラムを記録する。このような構成によれば、電子マネーカードに電子マネーをチャージするための端末を通常のコンピュータを用いて実現することができる。

【００３６】また、この発明の第８の観点にかかる媒体は、コンピュータを、カード利用者の身体の全体もしくは一部をスキャンするスキャン手段、前記スキャン手段によりスキャンしたデータを所定形式に変換する変換手段、電子マネー情報が記録されている媒体に記録されている利用者の身体的特徴に関する特徴データを読み取る読取手段、前記読取手段により読み取られたデータと前記変換手段により変換されたデータとを比較する手段、前記データの比較における一致度を判定する手段、上記

判定結果が一定値以上の場合、電子マネー取引を有効とする手段、として機能させるためのプログラムを記録する。

【００３７】

【発明の実施の形態】以下、この発明の実施の形態にかかる電子マネーシステムを図面を参照して説明する。この電子マネーシステムは、図１に示すように、センタ１０に配置されている認証局１１及び電子マネーサーバ１３と、電子マネー端末（取引装置）１５と、銀行センタ１７と、電子マネーカード１９と、より構成される。

【００３８】センタ１０は、この電子マネーシステム全体の動作、電子マネーの流通を制御（管理）するコンピュータシステムである。センタ１０の認証局１１は、この電子マネーシステムにおける利用者等に対して認証情報を生成する。認証局１１は、認証を行う際、利用者が登録されていることをチェックするため、このシステムにおいて使用される全ての電子マネーカード１９のカードＩＤ及び公開鍵を記憶する。

【００３９】認証局１１は、一対のセンタ秘密鍵Ck1とセンタ公開鍵Ck2を生成し、記憶する。認証局１１は、電子マネーサーバ１３にセンタ秘密鍵Ck1をコピーすることにより、センタ秘密鍵Ck1をセンタ１０内で共有化する。また、認証局１１は、センタ公開鍵Ck2を各電子マネー端末１５等に電子マネーサーバ１３を介して予め配布する。また、認証局１１は、後述する個人認証情報を生成するための署名鍵Skと、その署名鍵Skによってなされた署名、即ち、個人認証情報を確認するための検査鍵Ekとを生成、記憶し、検査鍵Ekを各電子マネー端末１５に予め配布しておく。

【００４０】電子マネーサーバ１３は、図２、図３に示すように、各電子マネーカード１９が保持する電子マネーの残高を示す残高テーブル、使用不可になった電子マネーカード１９のカードＩＤのリスト（事故カードリスト）、使用不可になった電子マネー端末１５の端末ＩＤのリスト（事故端末リスト）、電子マネーの取引の履歴のリスト（取引履歴テーブル）を記憶する。

【００４１】電子マネーサーバ１３は、電子マネーの取引を行うため、これらの記憶データを用いて、認証局１１への認証要求、銀行センタ１７への振替要求、各電子マネーカード１９及び電子マネー端末１５の制御・管理等を行う。

【００４２】電子マネー端末１５は、利用者が電子マネーカード１９を挿入又は装着し、所定の操作をすることにより、電子マネーの取引をするための端末である。電子マネー端末１５には、電子マネーを電子マネーカード１９に補充（チャージ）するためのチャージ端末（ＡＴＭ等）、電子マネーカード相互間の電子マネーの授受を処理する端末、店舗等に配置され、物品やサービスの売り上げ金額に相当する電子マネーを受領するＰＯＳ端末、自動販売機等がある。１つの端末が電子マネーに関

する複数の機能、例えば、ＡＴＭ機能とＰＯＳ機能を備えている場合もある。

【００４３】各電子マネー端末１５は、記憶部３０と、入力部３１と、表示部３２と、カード処理部３３とを備える。

【００４４】記憶部３０は、その電子マネー端末１５に付与された端末ＩＤ、前述の認証局１１より供給された個人認証情報確認用の検査鍵Ek及びセンタ公開鍵Ck2、一対の端末秘密鍵Tk1と端末公開鍵Tk2とセンタ１０とのオフライン時の電子マネーの取引履歴等を格納する。

【００４５】入力部３１は、電子マネー取引の指示を入力する。表示部３２は、処理メニュー、メッセージ等を表示する。カード処理部３３は、電子マネーカード１９を受け付ける挿入口と、電子マネーカード１９のＩＣ部２０をアクセスするためのＩＣリード／ライト部と、光記憶部２１をアクセスするための光記憶リード／ライト部とを備える。

【００４６】図４（Ａ）にＡＴＭ型の電子マネー端末１５の例を示す。この電子マネー端末１５の入力部３１と表示部３２は、タッチパネル型の表示部３４から構成され、カード処理部３３は、電子マネーカード１９が挿入されるカード挿入口３５Ａと３５Ｂを備える。カード挿入口３５Ａは、通常の処理と電子マネーの譲渡の際の譲渡元のカードが挿入される。カード挿入口３５Ｂは、電子マネーの譲渡の際の譲渡先のカードが挿入される。

【００４７】図４（Ｂ）にＰＯＳ型の電子マネー端末の例を示す。この電子マネー端末１５の入力部３１は、電子マネーの取引の指示等と共に売り上げ金額額などを入力するためのキーボード３１Ａとバーコードリーダ３１Ｂ等を含む。また、表示部３２は、電子マネー取引のためメッセージ等と共に売り上げ金額などを表示し、顧客用の表示部３２Ａと操作者用の表示部３２Ｂを備える。また、カード処理部３３はカード挿入口３５を備える。さらに、ＰＯＳ用に金銭ドロア３６等も配置されている。

【００４８】銀行センタ１７は、電子マネーカード１９の利用者（保有者）の口座である決済口座と銀行が保有する電子マネーの運用口座である別段口座を備え、これらの口座の入出金処理を行う。例えば、銀行センタ１７は、センタ１０からの指示に応じて電子マネーカード１９に対応する決済口座から別段口座への振り替え及び別段口座から決済口座への振り替えを行う。この振り替え処理を行うため、銀行センタ１７は、各電子マネーカード１９に付与されているカードＩＤと各電子マネーカード１９の利用者（保有者）の決済口座の口座番号を対応させる口座テーブルを図５に示すように記憶する。

【００４９】電子マネーカード１９は、図６に示すように、ＩＣ部（ＩＣチップ）２０と光記憶部２１を備える光ＩＣハイブリッドカードから構成される。なお、電子

マネーカード１９は、ＩＣ部（ＩＣチップ）２０と光記憶部２１を備えていればよく、その形状はカード型に限定されず任意である。

【００５０】ＩＣ部２０は制御回路とメモリ回路を内蔵する。このメモリ回路は、図６に示すように、動作プログラムの他に、カードＩＤ、個人秘密鍵Ｐk1、個人公開鍵Ｐk2、電子マネーの残高、後述するオンライン取引用の個人認証情報、等を記憶する。また、ＩＣ部２０は、後述する光記憶部２１に記憶される取引履歴のうち、最終的な取引履歴の位置を示す最終取引ポインタと、電子マネーサーバ１３へ最後に送信した取引履歴の位置を示す送信済みポインタを記憶する。

【００５１】光記憶部２１は、例えば、光エネルギーが照射されることによりピット等が形成されてデータが書き込まれるタイプの書き換え不可能な追記型の記憶媒体等から構成され、電子マネーカード１９で取り引きされた電子マネーの取引履歴を順次記憶する。

【００５２】取引履歴を構成する項目としては、電子マネーの取引の種別を示す利用区分（チャージ（残高の補充）、支払、譲渡、換金等）、取引のために電子マネーカードが装着された電子マネー取引端末１５の端末ＩＤ、電子マネーカード１９間の電子マネーの授受の場合には相手のカードＩＤ、利用年月日、取引金額、認証子（上記項目と個人秘密鍵Ｐk1を用いて作成した取引認証子、上記項目と取引相手（電子マネー端末１５又は他の電子マネーカード１９）の秘密鍵Ｐk1を用いて作成した取引先認証子）、等がある。

【００５３】このような構成を有する電子マネーシステムにおける基本的な処理には、（１）電子マネーチャージ処理（電子マネーカード１９に記憶される残高の補充）、（２）個人認証情報発行処理、（３）電子マネー支払い処理、（４）突き合わせ処理、（５）電子マネー譲渡処理、（６）電子マネー換金処理、等がある。これらの処理について、以下順番に説明する。

【００５４】（１）　電子マネーチャージ処理

電子マネーチャージ処理を図７を参照して説明する。ＡＴＭ機能を備える電子マネー端末１５は、図８（Ａ）に示すように、処理選択メニューを表示している。利用者は、表示部３２（タッチパネル３４）に表示されている処理メニューの中から「１）電子マネーのチャージ」を選択する。

【００５５】この選択に応答し、電子マネー端末１５は、図８（Ｂ）に示すように、電子マネーカード１９をカード挿入口３５Ａに挿入すべき旨のメッセージを表示する。

【００５６】電子マネー端末１５は、電子マネーカード１９が挿入されると、図８（Ｃ）に示すようなチャージ金額入力画面を表示し、利用者は入力部３１（タッチパネル３４）から所望のチャージ金額を入力する。チャージ金額が入力されると電子マネー端末１５は、電子マネーカード１９に、取引区分（チャージ）と利用年月日と取引金額（チャージ金額）とから構成される取引情報と端末ＩＤを送信するとともに、カードＩＤと個人公開鍵Ｐk2の送信を要求する要求信号を送信する（Ｐ１）。

【００５７】電子マネーカード１９のＩＣ部２０は、端末ＩＤと取引情報に、カードＩＤを加え、これらの情報を個人秘密鍵Ｐk1を用いて取引認証子｛Ｐk1（端末ＩＤ＋取引情報＋カードＩＤ）｝に変換し、その取引認証子とカードＩＤと個人公開鍵Ｐk2とを電子マネー端末１５に送信する（Ｐ２）。

【００５８】電子マネー端末１５は、受信したカードＩＤに取引情報と端末ＩＤ加え、端末秘密鍵Ｔk1を用いて取引先認証子｛Ｔk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を作成する。電子マネー端末１５は、作成した取引先認証子｛Ｔk1（端末ＩＤ＋取引情報＋カードＩＤ）｝と、要求された金額のチャージを指示し、端末公開鍵Ｔk2を含むチャージ要求電文と、電子マネーカード１９のカードＩＤと、個人公開鍵Ｐk2と、取引認証子とを電子マネーサーバ１３に送信する（Ｐ３）。なお、チャージ要求電文は、送信元の電子マネー端末１５の端末ＩＤを含む。

【００５９】電子マネーサーバ１３は、受信したカードＩＤ及び端末ＩＤが、記憶部３０に記憶している事故カードリスト（図２（Ｂ））及び事故端末リスト（図２（Ｃ））に登録されているか否かを判別する。受信したカードＩＤ及び端末ＩＤが、これらのリストに登録されていないと判別された場合、電子マネーサーバ１３は、受信した個人公開鍵Ｐk2を用いて取引認証子｛Ｐk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を端末ＩＤと取引情報とカードＩＤとに変換する。又、受信した端末公開鍵Ｔk2を用いて取引先認証子｛Ｔk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を端末ＩＤと取引情報とカードＩＤに変換する。さらに、取引認証子から変換された端末ＩＤと取引情報とカードＩＤと、取引先認証子から変換された端末ＩＤと取引情報とカードＩＤとが一致するか否かを判別する。これらが一致した場合、電子マネーサーバ１３は、この取引認証子と取引先認証子は正しいと判別し、そのカードＩＤに対応する決済口座から銀行センタ１７の別段口座へ指示された金額を移動する（出金する）よう指示する出金電文を銀行センタ１７に送信する（Ｐ４）。

【００６０】なお、受信したカードＩＤと端末ＩＤの少なくとも一方が事故カードリスト及び事故端末リストに登録されている場合、又は取引認証子と取引先認証子から変換された端末ＩＤと取引情報とカードＩＤとの少なくとも一部が一致しない場合、電子マネーサーバ１３は、電子マネー端末１５にチャージ不可を指示するメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者等に通知する。電子マネー端末１５はチャージをできない旨のメッセージを表示部３２に表示す

る。

【００６１】銀行センタ１７は、電子マネーサーバ１３より、出金電文を受信すると、図５に示す口座テーブルを参照して、カードＩＤに対応する口座番号を判別する。次に、この口座番号の決済口座の残高をチェックし、残高が指示された金額以上であるか否かを判別する。残高が指示された金額以上であると判別した場合、出金可能と判別し、決済口座から別段口座に指示された所定金額を移動する（振り替える）（Ｐ５）。次に、振替完了を通知する出金完了電文を電子マネーサーバ１３に送信する（Ｐ６）。

【００６２】決済口座の残高の不足により出金不可能な場合には、銀行センタ１７は、チャージ不可を指示する電文を電子マネーサーバ１３に送信する。電子マネーサーバ１３はチャージ処理を中止すると共に電子マネー端末１５に同様のメッセージを送信する。電子マネー端末１５はこのメッセージに応答して、その旨を示すメッセージを表示部３２等に表示する。

【００６３】電子マネーサーバ１３は、出金完了電文を銀行センタ１７から受信すると、記憶部３０に記憶していた電子マネーカード１９のカードＩＤ及び個人公開鍵Ｐk2を認証局１１へ送信し、それらに対する認証情報を要求する（Ｐ７）。認証局１１は、自己が記憶するカードＩＤ及び個人公開鍵Ｐk2のリストに、受信したカードＩＤ及び個人公開鍵Ｐk2が登録されているかをチェックする。それらが登録されているならば、認証局１１は、センタ秘密鍵Ck1を用いて、受信したカードＩＤ及び個人公開鍵Ｐk2を認証情報｛Ck1（カードＩＤ＋Ｐk2）｝に変換し、認証完了電文と共に電子マネーサーバ１３へ返送する（Ｐ８）。

【００６４】電子マネーサーバ１３は、認証完了電文及び認証情報｛Ck1（カードＩＤ＋Ｐk2）｝を受信すると、図２（Ａ）に示す残高テーブル上で、電子マネーカード１９にチャージされている電子マネーの残高を示す残高データを更新する。さらに、図３に示すように、取引情報（利用区分（チャージ）、利用年月日、取引金額）とカードＩＤと端末ＩＤと認証子（取引認証子と取引先認証子）より構成される今回の取引履歴を過去の取引履歴に追加して記憶する。次に、電子マネーサーバ１３は、認証局１１からの認証情報を今回の取引履歴に付与し、チャージの完了を示すチャージ完了電文と共に電子マネー端末１５に送信する（Ｐ９）。

【００６５】電子マネー端末１５は、取引履歴と認証情報を受信すると、センター公開鍵Ck2を用いて認証情報をカードＩＤと個人公開鍵Ｐk2に変換し、チェックする。その認証情報が正しいものであると確認すると、受信した取引履歴に基づいて、ＩＣ部２０の制御部を介して、ＩＣ部２０のメモリエリアに記録されている残高を更新する。

【００６６】また、電子マネー端末１５は、ＩＣ部２０より最終取引ポインタを読み出し、最終取引ポインタが指示する位置の次のアドレス位置に今回の取引履歴｛取引情報（利用区分（チャージ）、利用年月日、取引金額）とカードＩＤと端末ＩＤと認証子（取引認証子と取引先認証子）｝を過去の取引履歴に追加して記憶する。さらに、電子マネー端末１５は、ＩＣ部２０の制御部を介して、ＩＣ部２０のメモリエリアに記録されている最終取引ポインタ及び送信済みポインタが追記した取引履歴の位置を指すように更新する（Ｐ１０）。その後、端末１５はチャージが完了した旨を表示部３２に表示すると共に電子マネーカード１９を排出する。

【００６７】この電子マネーチャージ処理を、利用者Ａが、電子マネー端末１５Ｂ（端末ＩＤ”Ｔ１５０”）を用いて、自己の電子マネーカード１９Ａ（カードＩＤ”Ｃ９９”）に１万円分の電子マネーをチャージする場合を例に、図９を参照して説明する。まず、利用者Ａは、表示部３２に表示された処理メニューから「１）電子マネーのチャージ」を選択し、電子マネーカード１９Ａを電子マネー端末１５Ｂに挿入し、チャージ金額として「１万円」を入力する。

【００６８】電子マネー端末１５Ｂは、この入力に応答し、取引区分（チャージ）と利用年月日と取引金額とから構成される取引情報と端末ＩＤ”Ｔ１５０”とを、カードＩＤと個人公開鍵Ｐk2を要求する要求信号と共に電子マネーカード１９Ａに送信する（Ｌ１）。

【００６９】電子マネーカード１９Ａは、受信した端末ＩＤ”Ｔ１５０”と取引情報にカードＩＤ”Ｃ９９”を加え、個人秘密鍵Ｐk1Ａを用いて取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝を作成する。電子マネーカード１９Ａは、作成した取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝をカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａと共に電子マネー端末１５Ｂに送信する（Ｌ２）。

【００７０】電子マネー端末１５Ｂは、カードＩＤ”Ｃ９９”と記憶部３０に記憶していた取引情報に端末ＩＤを加え、端末秘密鍵Tk1Ｂを用いて取引先認証子｛Tk1Ｂ（Ｔ１５０＋取引情報＋Ｃ９９）｝を作成する。電子マネー端末１５Ｂは、作成した取引先認証子｛Tk1Ｂ（Ｔ１５０＋取引情報＋Ｃ９９）｝と、１万円分の電子マネーのチャージを要求すると共に端末ＩＤ”Ｔ１５０”と端末公開鍵Tk2Ｂとを含むチャージ要求電文と、電子マネーカード１９Ａのカードｉｄ”Ｃ９９”と、個人公開鍵Ｐk2Ａと、取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝とを、電子マネーサーバ１３に送信する（Ｌ３）。

【００７１】電子マネーサーバ１３は、受信した端末ＩＤ”Ｔ１５０”とカードＩＤ”Ｃ９９”が、事故端末リスト及び事故カードリストに登録されているか否かを判別することにより、電子マネー端末１５及び電子マネーカード１９の不正使用をチェックする。

【００７２】チェックの結果、電子マネーカード１９Ａ及び電子マネー端末１５Ｂが事故カードと事故端末のいずれでもないと判別されたならば、電子マネーサーバ１３は、個人公開鍵Ｐk2Ａを用いて取引認証子を端末ＩＤと取引情報とカードＩＤとに変換する。又、端末公開鍵Ｔk2Ｂを用いて取引先認証子を端末ＩＤと取引情報とカードＩＤとに変換する。次いで、取引認証子から変換された端末ＩＤと取引情報とカードＩＤと、取引先認証子から変換された端末ＩＤと取引情報とカードＩＤとが一致するか否かを判別する。これらが一致した場合、電子マネーサーバ１３は、この取引認証子と取引先認証子は正しいと判別し、銀行センタ１７へカードＩＤ”Ｃ９９”の決済口座から銀行センタ１７の別段口座へ１万円を移動するよう指示する出金電文を送信する（Ｌ４）。

【００７３】電子マネーカード１９Ａと電子マネー端末１５Ｂの両方又は一方が事故カード又は事故端末であると判別された場合、及び／又は、取引認証子と取引先認証子から変換された端末ＩＤと取引情報とカードＩＤとが互いに一致しない場合、電子マネーサーバ１３は、電子マネー端末１５Ｂにチャージできない旨のメッセージを送信すると共に、不正又は異常の検出を管理者に通知する。

【００７４】銀行センタ１７は、出金電文を受信すると、図５に示す口座テーブルを参照してカードＩＤ”Ｃ９９”の決済口座の口座番号”３０００００１”を検索し、該当する口座番号の残高が、指示されたチャージ金額の１万円以上か否かを判別する。残高が１万円未満の場合は、銀行センタ１７は、残高不足のためチャージできないの旨の電文を電子マネーサーバ１３に送信する。残高が１万円以上の場合、銀行センタ１７は、決済口座”３０００００１”から銀行センタ１７の別段口座へ１万円を移動し、出金完了電文を電子マネーサーバ１３に送信する（Ｌ５）。

【００７５】電子マネーサーバ１３は、銀行センタ１７から出金完了電文を受信すると、電子マネーカード１９ＡのカードＩＤと個人公開鍵Ｐk2Ａに対して認証を要求する認証付与要求を、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａと共に認証局１１へ送信する（Ｌ６）。

【００７６】認証局１１は、自己が記憶している電子マネーカード１９ＡのカードＩＤ及び個人公開鍵Ｐk2のリストに、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａが存在する（即ち、認証局１１に登録されている）ことをチェックする。カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａとが認証局１１に登録されている場合、認証局１１は、センタ秘密鍵Ｃk1を用いて、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａに対する認証情報｛Ｃk1（Ｃ９９＋Ｐk2Ａ）｝を生成し、認証の完了を示す認証完了電文と共に電子マネーサーバ１３に送信する（Ｌ７）。

【００７７】電子マネーサーバ１３は、認証完了電文を受信すると、利用区分”チャージ”、利用年月日、カードＩＤ”Ｃ９９”、端末ＩＤ”Ｔ１５０”、チャージ金額”１万円”、取引認証子、取引先認証子、等により取引履歴を生成して図３に示すように記憶する。また、図２（Ａ）に示す残高テーブルのカードＩＤ”Ｃ９９”の残高に１万円加算する。さらに、生成した取引履歴に認証局１１からの認証情報を付与して、チャージ完了電文と共に電子マネー端末１５Ｂに送信する（Ｌ８）。

【００７８】電子マネー端末１５Ｂは、認証情報が付与された取引履歴を受信すると、センター公開鍵Ｃk2を用いて認証情報｛Ｃk1（Ｃ９９＋Ｐk2Ａ）｝をカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａに変換し、チェックする。その、その認証情報が正しいものであると確認すると、受信した取引履歴を電子マネーカード１９ＡのＩＣチップ２０に送信する（Ｌ９）。ＩＣチップ２０は、受信した取引履歴に基づいて、自己が記憶している残高に１万円を加算する。

【００７９】また、電子マネー端末１５Ｂは、ＩＣチップ２０から最終取引ポインタを読み出し、光記憶部２１の最終取引ポインタが示す位置の次の位置に取引履歴を追記し、最終取引ポインタ及び送信済みポインタを追記された取引履歴を示すように更新する。その後、端末１５Ｂはチャージが完了した旨を表示部３２に表示すると共に電子マネーカード１９Ａを排出する。このようして、利用者Ａは自己の電子マネーカード１９Ａに、１万円分の電子マネーをチャージすることができる。

【００８０】（２）個人認証情報発行処理

次に、電子マネーカード１９のＩＣ部２０に記憶される個人認証情報の発行処理（個人認証情報発行処理）について説明する。後述するオフラインによる電子マネー支払い処理において、電子マネーカード１９は、この個人認証情報を電子マネー端末１５に提示し、電子マネー端末１５によりその個人認証情報の確認を受けることで、取引することが可能となる。個人認証情報は、電子マネーカード１９のカードＩＤ及び個人公開鍵Ｐk2をもとに作成されるため、個人秘密鍵Ｐk1及び個人公開鍵Ｐk2が変更される度に取得される必要がある。

【００８１】図１０に個人認証情報発行処理の概要図を示す。まず、図８に示すように、表示部３２に表示される処理メニューから「４）個人認証情報の発行」が選択され、電子マネーカード１９が電子マネー端末１５に挿入される。電子マネー端末１５は、この操作に応答して、電子マネーカード１９のＩＣ部２０にカードＩＤと個人公開鍵Ｐk2の要求を示す要求信号を送信する（Ｐ１１）。

【００８２】この要求信号に応答して、電子マネーカード１９のＩＣチップ２０は、カードＩＤと個人公開鍵Ｐk2を電子マネー端末１５に送信する（Ｐ１２）。電子マネー端末１５は、受信したカードＩＤと個人公開鍵Ｐk2とを、個人認証情報を要求する認証情報発行要求と共に

電子マネーサーバ１３に送信する（Ｐ１３）。なお、認証情報発行要求は端末ＩＤを含む。

【００８３】電子マネーサーバ１３は、電子マネー端末１５からカードＩＤと個人公開鍵Ｐk2と認証情報発行要求を受信すると、受信したカードＩＤ及び端末ＩＤが事故カードＩＤリスト及び事故端末ＩＤリストに登録されているか否かチェックする。

【００８４】チェックの結果、受信したカードＩＤと端末ＩＤの少なくとも一方が事故カードＩＤリスト又は事故端末ＩＤリストに登録されている場合、電子マネーサーバ１３は、電子マネー端末１５に個人認証情報を発行できない旨のメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者に通知する。電子マネー端末１５はこのメッセージを表示する。

【００８５】受信したカードＩＤ及び端末ＩＤが事故カードＩＤリスト及び事故端末ＩＤリストに登録されていない場合、電子マネーサーバ１３は、受信したカードＩＤと個人公開鍵Ｐk2と個人認証情報の発行要求（個人認証情報発行要求）を認証局１１に送信する（Ｐ１４）。

【００８６】認証局１１は、電子マネーサーバ１３からカードＩＤと個人公開鍵Ｐk2と個人認証情報発行要求を受信すると、自己が記憶するカードＩＤ及び個人公開鍵のリストを参照することにより、受信したカードＩＤ及び個人公開鍵が本システムにおいて使用可能なものとして登録されているか否かをチェックする。登録されていない場合、認証局１１はその旨の電文を電子マネーサーバ１３に送信する。電子マネーサーバ１３は、電子マネー端末１５に同様の電文を送信する。電子マネー端末１５はこのメッセージを表示する。

【００８７】一方、受信したカードＩＤと個人公開鍵Ｐk2が登録されている場合、認証局１１は個人認証情報生成用の署名鍵Ｓkを用いて個人認証情報｛Ｓk（カードＩＤ＋Ｐk2）｝を生成し、発行完了電文と共に電子マネーサーバ１３に送信する（Ｐ１５）。

【００８８】電子マネーサーバ１３は、認証局１１からの個人認証情報｛Ｓk（カードＩＤ＋Ｐk2）｝と発行完了電文を電子マネー端末１５へ送信する（Ｐ１６）。電子マネー端末１５は、受信した個人認証情報｛Ｓk（カードＩＤ＋Ｐk2）｝を電子マネーカード１９のＩＣ部２０へ送信する（Ｐ１７）。ＩＣ部２０は、受信した個人認証情報｛Ｓk（カードＩＤ＋Ｐk2）｝を記憶回路に記憶する。その後、電子マネー端末１５は、個人認証情報の取得が完了した旨を表示部３２に表示すると共に電子マネーカード１９を排出する。

【００８９】この個人認証情報発行処理を、例えば、利用者Ａが電子マネーカード１９Ａ（カードＩＤ”Ｃ９９”）の個人認証情報を取得する場合を例に、図１１を参照して説明する。

【００９０】まず、利用者Ａは、表示部３２に表示されたメニューの中から「４）個人認証情報の発行」を選択し、電子マネーカード１９Ａを電子マネー端末１５Ｂに挿入する。電子マネー端末１５Ｂは、この操作に応答し、電子マネーカード１９Ａにカードの送信を要求する要求信号を送信する（Ｌ１１）。

【００９１】電子マネーカード１９ＡのＩＣ部２０は、電子マネー端末１５Ｂからの要求信号を受信すると、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを電子マネー端末１５Ｂに送信する（Ｌ１２）。電子マネー端末１５Ｂは、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを認証情報発行要求と共に電子マネーサーバ１３に送信する（Ｌ１３）。

【００９２】電子マネーサーバ１３は、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａとが、事故カードＩＤリスト及び事故端末ＩＤリストに登録されているか否かを判別することにより、電子マネーカード１９及び電子マネー端末１５の不正使用をチェックする。不正使用と判別された場合、電子マネーサーバ１３は、電子マネー端末１５Ｂに個人認証情報を発行できない旨のメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者に通知する。電子マネー端末１５Ｂは、このメッセージを表示する。

【００９３】チェックの結果、電子マネーカード１９Ａ及び電子マネー端末１５Ｂが使用可能ならば、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを個人認証情報発行要求と共に認証局１１へ送信する（Ｌ１４）。

【００９４】認証局１１は、電子マネーサーバ１３から受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａに署名鍵Ｓkを用いてデジタル署名を施すことにより個人認証情報｛Ｓk（Ｃ９９＋Ｐk2Ａ）｝を生成し、発行完了電文と共に電子マネーサーバ１３に送信する（Ｌ１５）。

【００９５】電子マネーサーバ１３は、認証局１１からの個人認証情報｛Ｓk（Ｃ９９＋Ｐk2Ａ）｝と発行完了電文を電子マネー端末１５に送信する（Ｌ１６）。電子マネー端末１５は、電子マネーサーバ１３から受信した個人認証情報を電子マネーカード１９Ａに送信する（Ｌ１７）。電子マネーカード１９ＡのＩＣ部２０は、電子マネー端末１５から受信した個人認証情報を記憶する。その後、電子マネー端末１５Ｂは、個人認証情報の取得が完了した旨を表示部３２に表示すると共に電子マネーカード１９Ａを排出する。

【００９６】個人認証情報は、個人秘密鍵Ｐk1及び個人公開鍵Ｐk2が電子マネー端末１５で変更された際に、自動的に該電子マネー端末１５を介して取得されてもよい。

【００９７】（３）　電子マネー支払い処理

次に、電子マネー支払い処理について図１２を参照して説明する。この処理は、例えば、店舗等において商品、サービス等を購入し、その料金を電子マネーで支払うための処理である。電子マネー端末１５は、例えば、図４

（Ｂ）に示すようなＰＯＳ端末、自動販売機、等の形態をとる。

【００９８】例えば、ＰＯＳ端末型電子マネー端末１５で売り上げ額を計算した後、支払い方法を選択する旨のメッセージが表示部３２に表示される。ここで、電子マネーカードによる支払いが選択されると、電子マネーカード１９を挿入する旨の指示が表示され、電子マネーカード１９が電子マネー端末１５に挿入される。

【００９９】電子マネー端末１５は、電子マネーカード１９の挿入に応答して、取引区分と利用年月日と取引金額（支払い金額）とから構成される取引情報と端末ＩＤと、カードＩＤと個人公開鍵Ｐk2と個人認証情報｛Ｓk（カードＩＤ＋Ｐk2）｝と残高の送信を要求する要求信号を電子マネーカード１９に送信する（Ｐ２１）。

【０１００】電子マネーカード１９のＩＣ部２０は、受信した端末ＩＤ及び取引情報にカードＩＤを加え、個人秘密鍵Ｐk1を用いて取引認証子｛Ｐk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を作成する。ＩＣ部２０は、作成した取引認証子｛Ｐk1（端末ＩＤ＋取引情報＋カードＩＤ）｝をカードＩＤと個人公開鍵Ｐk2と個人認証情報｛Ｓk（カードＩＤ＋Ｐk2）｝と残高とを電子マネー端末１５に送信する（Ｐ２２）。

【０１０１】電子マネー端末１５は、電子マネーカード１９からカードＩＤと個人公開鍵Ｐk2と個人認証情報｛Ｓk（カードＩＤ＋Ｐk2）｝と残高と取引認証子｛Ｐk2（端末ＩＤ＋取引情報＋カードＩＤ）｝を受信すると、まず、個人認証情報｛Ｓk（カードＩＤ＋Ｐk2）｝を検査鍵Ｅkを用いて、カードＩＤと個人公開鍵Ｐk2に変換し、これらが電子マネーカード１９から受信したカードＩＤと個人公開鍵Ｐk2とに一致するか否かを判別する。一致しない場合、電子マネー端末１５は、何からの不正があると判断し、取引不可のメッセージを表示し、不正検出を電子マネーサーバ１３に通知する。

【０１０２】電子マネー端末１５は、個人認証情報から復号されたカードＩＤと個人公開鍵Ｐk2が、電子マネーカード１９から受信したカードＩＤと個人公開鍵Ｐk2に一致すると判断すると、受信した残高が支払金額以上か否かを判別する。残高が支払い金額以上ならば、支払可能と判断し、取引情報とカードＩＤと端末ＩＤに対して端末秘密鍵Ｔk1を用いて取引先認証子｛Ｔk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を生成する。電子マネー端末１５は、取引情報とカードＩＤと端末ＩＤと取引認証子｛Ｐk2（端末ＩＤ＋取引情報＋カードＩＤ）｝と取引先認証子｛Ｔk1（端末ＩＤ＋取引情報＋カードＩＤ）｝より取引履歴を構成し、支払い完了電文と共に電子マネーカード１９に送信し（Ｐ２３）、さらに、自己の記憶部３０にも記憶する。

【０１０３】電子マネーカード１９のＩＣ部２０は、受信した取引履歴に基づいて、記憶回路に格納している残高を更新すると共に最終履歴ポインタの値を電子マネー

端末１５に転送する。電子マネー端末１５は、電子マネーカード１９の光記憶部２１の最終履歴ポインタが指示するアドレスの次のアドレスに取引履歴を書き込むと共にＩＣ部２０に最終履歴ポインタを更新するコマンドを送出する。このコマンドに応答して、ＩＣ部２０は記憶回路に格納されている最終取引ポインタの値を更新する。ただし、送信済みポインタの値を更新しない。その後、電子マネー端末１５は、支払いが完了した旨を表示すると共に電子マネーカード１９を排出する。

【０１０４】上述したように、この電子マネー支払い処理は、電子マネーカード１９と電子マネー端末１５の間で処理されるオフライン処理である。これにより、処理速度を向上し、レスポンスを速くし、顧客の待ち時間等を短縮することができる。

【０１０５】電子マネー端末１５は、所定のタイミングで電子マネーサーバ１３と通信を行い、記憶部３０に蓄積していた取引履歴を送信する。電子マネーサーバ１３は、受信した取引履歴を図３に示すように、取引履歴テーブルに記憶する。電子マネー端末１５が取引履歴を電子マネーサーバ１３に送信するタイミングとしては、例えば、電子マネー支払い処理が完了した直後等のタイミングが望ましい。しかし、これに限定されるものではなく、たとえば、一定期間毎（例えば、１０分毎）、電子マネーサーバ１３からのポーリングに応じて等、任意である。

【０１０６】電子マネー端末１５は、記憶部３０に蓄積していた取引履歴を電子マネーサーバ１３に送信した後、送信済みの取引履歴を消去してもよく、又、送信済みフラグ等を付与することにより、送信済みの取引履歴と未送信の取引履歴とを区別して管理してもよい。

【０１０７】電子マネー支払い処理を、例えば、利用者Ａが、端末ＩＤが”Ｔ１５０”の電子マネー端末１５Ｂが設定された店舗において１万円の商品を購入し、その支払いを電子マネーカード１９Ａ（カードＩＤ”Ｃ９９”）で行う場合を例に図１３を参照して説明する。まず、電子マネー端末１５Ｂ（例えばＰＯＳ端末）の表示部３２に金額”１万円”が支払金額として表示され、利用者が電子マネーによる支払いを選択したとする。まず、利用者Ａ又は店員が電子マネーカード１９Ａを電子マネー端末１５Ｂに挿入する。

【０１０８】電子マネー端末１５Ｂは、電子マネーカード１９Ａの挿入に応答して、取引区分と取引年月日と取引金額とから構成される取引情報と端末ＩＤ”Ｔ１５０”と、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2と個人認証情報と残高の送信を要求する要求信号を電子マネーカード１９Ａに送信する（Ｌ２１）。

【０１０９】電子マネーカード１９Ａは、受信した端末ＩＤ”Ｔ１５０”と取引情報にカードＩＤ”Ｃ９９”を加え、個人秘密鍵Ｐk1Ａを用いて取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝を作成する。電子マ

ネーカード１９Ａは、作成した取引認証子｛Ｐk2Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝と、カードＩＤ”Ｃ９９”と、個人公開鍵Ｐk2Ａと、個人認証情報｛Ｓk（Ｃ９９＋Ｐk2）｝と、残高とを電子マネー端末１５に送信する（Ｌ２２）。

【０１１０】電子マネー端末１５Ｂは、電子マネーカード１９Ａから、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａと個人認証情報｛Ｓk（カードＩＤ＋Ｐk2）｝と残高と取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝とを受信し、個人認証情報｛Ｓk（Ｃ９９＋Ｐk2）｝を、予め記憶している検査鍵Ekを用いてカードＩＤと個人公開鍵Ｐk2Ａに変換する。次に、個人認証情報から復号されたカードＩＤと個人公開鍵Ｐk2Ａが、電子マネーカード１９Ａのカードｉｄ”Ｃ９９”と個人公開鍵Ｐk2Ａと一致することを確認する。

【０１１１】次に、電子マネー端末１５Ｂは、電子マネーカード１９Ａの残高が支払い金額（この場合１万円）以上か否かを判別する。残高が１万円以上ならば、電子マネー端末１５Ｂは、端末ＩＤ”Ｔ１５０”と取引情報とカードＩＤ”Ｃ９９”に対して端末秘密鍵Tk1Ｂを用いて取引先認証子｛Tk1Ｂ（Ｔ１５０＋取引情報＋Ｃ９９）｝を生成する。さらに、端末ＩＤ”Ｔ１５０”と取引情報とカードＩＤ”Ｃ９９”と取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝と取引先認証子｛Tk1Ｂ（Ｔ１５０＋取引情報＋Ｃ９９）｝より取引履歴を構成し、支払い完了電文と共に電子マネーカード１９Ａへ送信する（Ｌ２３）。また、取引履歴を自己の記憶部３０にも記憶する。その後、電子マネー端末１５Ｂは、支払いが完了した旨を表示すると共に電子マネーカード１９Ａを排出する。

【０１１２】電子マネーカード１９ＡのＩＣ部２０は、電子マネー端末１５Ｂから受信した取引履歴に基づいて、残高を１万円分減算すると共に最終取引ポインタの値を電子マネー取引端末１５Ｂに送信する。電子マネー取引端末１５Ｂは、光記憶部２１の最終取引ポインタが示すアドレスの次のアドレスに取引履歴を格納する。その後、ＩＣ部２０に最終読み出しポインタの値を次のアドレス位置を示すように更新する。ただし、送信済みポインタの値は更新しない。

【０１１３】一方、電子マネー端末１５Ｂが、個人認証情報｛Ｓk（カードＩＤ＋Ｐk2）｝から変換されたカードＩＤと個人公開鍵Ｐk2が電子マネーカード１９Ａのカードｉｄ”Ｃ９９”と個人公開鍵Ｐk2Ａと一致しないと判断した場合、電子マネー端末１５Ｂは電子マネーカード１９Ａを不正カードと判別し、支払い不可の旨のメッセージを表示部３２に表示すると共に、不正検出を電子マネーサーバ１３に通知する。また、電子マネーカード１９Ａの残高が１万円未満の場合、電子マネー端末１５Ｂは、残高不足のため支払い不可の旨のメッセージを表示部３２に表示する。

【０１１４】電子マネー端末１５Ｂは、記憶部３０に記憶していた取引履歴を支払い処理終了後、電子マネーサーバ１３に送信する。電子マネーサーバ１３は取引履歴を受信すると、受信した取引履歴を図３に示すように、取引履歴テーブルに格納する。電子マネー端末１５Ｂは、電子マネーサーバ１３から取引履歴の記憶部３０に蓄積していた取引履歴の送信完了後、送信済みの取引履歴を消去してもよく、又、送信済みフラグ等を付与することにより、送信済みの取引履歴と未送信の取引履歴とを区別して管理してもよい。

【０１１５】なお、以上の説明では、支払い処理をオフラインで行ったが、セキュリティを高めるため、取引金額が一定額以上の場合は、オンラインで処理するようにしてもよく、又、一回の取引限度額を定めてもよい。

【０１１６】（４）　突き合わせ処理

支払い処理等が実行されると、電子マネーカード１９には、電子マネーサーバ１３に対して未送信の取引履歴が発生する。これらの取引履歴は、オンラインで行われる処理（例えば、電子マネーのチャージ処理等）の実行時、その処理に先だって電子マネーサーバ１３に送信される。電子マネーサーバ１３は、電子マネーカード１９から取引履歴を電子マネー端末１５を介して受信すると、自己が記憶している取引履歴と突き合わせることにより、その正当性をチェックする。この突き合わせ処理の概要を図１４を参照して説明する。

【０１１７】電子マネーカード１９のＩＣ部２０は、電子マネー端末１５からの信号を受信すると、受信した信号が指示する処理の内容を判別し、それがオンライン処理を指示しているか否かを判別する。受信信号がオンライン処理を指示している際には、ＩＣ部２０は、他の処理を実行する前に、最終取引ポインタの値と送信済みポインタの値とが一致している否かを判別する。一致していないと判別した場合、ＩＣ部２０は、割り込み信号と共に、送信済みポインタが示すポインタの次の位置から、最終取引ポインタが示す位置までの各アドレスに記憶されている取引履歴とカードＩＤと個人公開鍵を電子マネー端末１５に送信する（Ｐ３１）。

【０１１８】例えば、「電子マネーのチャージ処理」が処理メニューの中から選択され、電子マネーカード１９が電子マネー端末１５に挿入され、金額が入力されると、電子マネー端末１５は、例えば、チャージ処理を行うために、取引情報等を電子マネーカード１９のＩＣ部２０に送信する（図７Ｐ１、図９のＬ１）。

【０１１９】ＩＣ部２０は、指示された処理がオンライン処理であることを取引情報から判別し、ＩＣ部２０の最終取引ポインタと送信済みポインタとが一致している否かを判別する。一致していないと判別した場合、ＩＣ部２０は、割り込み信号と共に、送信済みポインタが示すポインタの次の位置から、最終取引ポインタが示す位置までの各アドレスに記憶されている取引履歴とカード

ＩＤと個人公開鍵Ｐk2を電子マネー端末１５に送信する（Ｐ３１）。

【０１２０】電子マネー端末１５は、割り込み信号に応答し、受信したカードＩＤと個人公開鍵Ｐk2と取引履歴を電子マネーサーバ１３に送信する（Ｐ３２）。

【０１２１】電子マネーサーバ１３は、受信したカードＩＤと個人公開鍵Ｐk2を、それらが認証局１１に登録されていることの確認を要求する確認要求と共に認証局１１に送信する（Ｐ３３）。

【０１２２】認証局１１は、受信したカードＩＤと個人公開鍵Ｐk2が、自己が記憶するカードＩＤと個人公開鍵のリストに登録されているか否かを判別する。登録されていることを確認すると、確認の完了を示す確認完了電文を電子マネーサーバ１３に返送する（Ｐ３４）。受信したカードＩＤと個人公開鍵Ｐk2が登録されていない場合、認証局１１は、不正の検出を電子マネーサーバ１３に通知する。

【０１２３】認証局１１からの確認完了電文を受信すると、電子マネーサーバ１３は、電子マネーカード１９から受信した取引履歴を自己が記憶している取引履歴と突き合わせる。受信した取引履歴と自己が記憶している取引履歴が全て一致し、突き合わせが完了すると、電子マネーサーバ１３は、電子マネー端末１５に突き合わせ完了電文を送信する（Ｐ３５）。

【０１２４】電子マネー端末１５は、受信した突き合わせ完了電文を電子マネーカード１９に送信する（Ｐ３６）。電子マネーカード１９は、突き合わせ完了電文を受信すると、ＩＣ部２０に記憶している送信済みポインタを最終取引ポインタと一致するように更新する。続いて、電子マネー端末１５により本来要求されている処理を実行する。

【０１２５】電子マネーサーバ１３は、受信した取引履歴と自己が記憶している取引履歴が一致しないと判断した場合、電子マネー端末１５に突き合わせ不一致を通知すると共に、不正の検出をメッセージ表示等により管理者等に通知する。

【０１２６】なお、最終取引ポインタと送信済みポインタとが一致する場合、未送信履歴が存在しないため、電子マネーカード１９は、要求信号に応じた処理を続行する。

【０１２７】この突き合わせ処理を、電子マネー支払処理がなされた後でだけ実行するようにしてもよい。この場合、例えば、電子マネー端末１５は、電子マネー支払処理を実行すると、電子マネーカード１９のＩＣ部２０に未送信履歴フラグをセットする。電子マネー取引端末１５は、電子マネーカード１９が挿入され、オンライン処理が指示されると、未送信履歴フラグがオンであるか否かを判別し、オンならば、上述の突き合わせ処理を実行する。

【０１２８】この突き合わせ処理を、図１５、図１６を参照して具体的に説明する。ここで、利用者Ａは以前、カードＩＤ”Ｃ９９”の電子マネーカード１９Ａで電子マネーの支払いをしており、電子マネーカード１９Ａの光記憶部２１には未送信の取引履歴が記憶されていることとする。

【０１２９】利用者Ａは、例えば、電子マネーのチャージを指示し、電子マネーカード１９Ａを電子マネー端末１５Ｂに挿入する。電子マネー端末１５Ｂは、取引区分（チャージ）と利用年月日と取引金額とから構成される取引情報と端末ＩＤとを、カードＩＤと個人公開鍵Ｐk2を要求する要求信号と共に電子マネーカード１９ＡのＩＣ部２０に送信する。

【０１３０】ＩＣ部２０は、取引情報から、オンライン処理が選択されたことを判別し、内部に記憶している最終取引ポインタと送信済みポインタとが一致するか否かを判別する。図１６に示すように、送信済みポインタはアドレス”２”を指し、最終取引ポインタはアドレス”５”を示しているとすると、ＩＣ部２０は、送信済みポインタが指しているアドレス”２”の次のアドレス”３”から最終取引ポインタが指しているアドレス”５”までの取引履歴Ｒ３～Ｒ５を割り込み信号とカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａと共に電子マネー端末１５Ｂに送信する（Ｌ３１）。電子マネー端末１５Ｂは、受信した取引履歴Ｒ３～Ｒ５とカードＩＤと個人公開鍵Ｐk2Ａを電子マネーサーバ１３へ送信する（Ｌ３２）。

【０１３１】電子マネーサーバ１３は、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを確認要求と共に認証局１１に送信する（Ｌ３３）。認証局１１は、自己が記憶するカードＩＤと個人公開鍵のリストに、受信したカードＩＤと個人公開鍵Ｐk2Ａが登録されていることを確認し、確認完了電文を電子マネーサーバ１３に送信する（Ｌ３４）。

【０１３２】電子マネーサーバ１３は、確認完了電文を受信すると、取引履歴Ｒ３～Ｒ５と自己が記憶している取引履歴とを突き合わせる。即ち、アドレス”３”～”５”の取引履歴Ｒ３～Ｒ５が全て電子マネーサーバ１３に記憶されている取引履歴と一致することをチェックする。チェックの結果、取引履歴Ｒ３～Ｒ５が電子マネーサーバ１３に記憶されている取引履歴と一致するならば、電子マネーサーバ１３は、図２（Ａ）に示す残高テーブルのカードＩＤ”Ｃ９９”の残高を更新し、電子マネー端末１５Ｂに突き合わせ完了電文を送信する（Ｌ３５）。電子マネー端末１５Ｂは、受信した突き合わせ完了電文を電子マネーカード１９Ａに送信する（Ｌ３６）。電子マネーカード１９Ａは、突き合わせ完了電文を受信すると、図１６に示すように、ＩＣ部２０に記憶している送信済みポインタを”２”から”５”に更新する。

【０１３３】その後、電子マネー端末１５と電子マネー

カード１９Ａは指示されている電子マネーチャージ処理を実行する。

【０１３４】上述した突き合わせ処理では、電子マネーカード１９からの取引履歴と電子マネーサーバ１３に記憶されている電子マネー端末１５からの取引履歴を比較する。これにより、不正に生成された（例えば、取引金額が改竄された）取引履歴を容易に検出することができる。また、不正が検出された際、不正な電子マネーカード１９の光記憶部２１に記憶されている取引履歴を参照することにより、いつ、どこで、いくら使用されたか、等の使用履歴を知ることができる。

【０１３５】（５）　電子マネーの譲渡処理

次に、電子マネー譲渡処理の概要を図１７を参照して説明する。電子マネーを譲渡（移転）する側を電子マネーカード１９Ａとし、譲渡を受ける側を電子マネーカード１９Ｂとする。

【０１３６】図８に示す画面表示に従って、表示部３２に表示される処理メニューから「３）電子マネーの譲渡」が選択され、電子マネーカード１９Ａがカード挿入口３５Ａに電子マネーカード１９Ｂがカード挿入口３５Ｂにそれぞれ挿入され、電子マネーカード１９Ａから電子マネーカード１９Ｂへの譲渡金額が入力される。電子マネー端末１５は、この入力に応答して、電子マネーカード１９Ａと電子マネーカード１９Ｂに、取引区分（１９Ａから１９Ｂへの譲渡）と利用年月日と取引金額とから構成される取引情報と端末ＩＤと、カードＩＤと個人公開鍵の要求を示す要求信号をそれぞれ送信する（Ｐ４１）。

【０１３７】電子マネーカード１９Ａは、端末ＩＤ及び取引情報と要求信号を受信すると、個人秘密鍵Ｐk1Ａを用いて、端末ＩＤと取引情報と自己のカードＩＤに対する取引認証子｛Ｐk1Ａ（端末ＩＤ＋取引情報＋１９Ａのカードｉｄ）｝を作成する。電子マネーカード１９Ａは、作成した取引認証子とカードＩＤと個人公開鍵Ｐk2Ａとを電子マネー端末１５に送信する（Ｐ４２）。

【０１３８】また電子マネーカード１９Ｂは、端末ＩＤ及び取引情報と要求信号を受信すると、個人秘密鍵Ｐk1Ｂを用いて、端末ＩＤと取引情報と自己のカードＩＤに対する取引先認証子｛Ｐk1Ｂ（端末ＩＤ＋取引情報＋１９Ｂのカードｉｄ）｝を作成する。電子マネーカード１９Ｂは、作成した取引先認証子とカードＩＤと個人公開鍵Ｐk2Ｂとを電子マネー端末１５に送信する（Ｐ４２）。

【０１３９】電子マネー端末１５は、電子マネーカード１９Ａから受信した取引認証子｛Ｐk1Ａ（端末ＩＤ＋取引情報＋１９Ａのカードｉｄ）｝とカードＩＤと個人公開鍵Ｐk2Ａと、電子マネーカード１９Ｂから受信した取引先認証子｛Ｐk1Ｂ（端末ＩＤ＋取引情報＋１９Ｂのカードｉｄ）｝とカードＩＤと個人公開鍵Ｐk2Ｂと、電子マネーカード１９Ａから電子マネーカード１９Ｂに入力された金額（譲渡金額）を移動するよう指示する譲渡依頼電文とを、電子マネーサーバ１３に送信する（Ｐ４３）。なお、譲渡依頼電文は端末ＩＤを含む。

【０１４０】電子マネーサーバ１３は、受信した電子マネーカード１９Ａと電子マネーカード１９Ｂのカードｉｄ及び端末ＩＤが事故カードＩＤリスト及び事故端末ＩＤリストに登録されているか否かを判別する。

【０１４１】受信したカードＩＤ及び端末ＩＤが、事故カードＩＤリスト及び事故端末ＩＤリストに登録されていない場合、電子マネーサーバ１３は、図２（Ａ）に示す残高テーブルの電子マネーカード１９Ａの残高をチェックする。残高が不足している場合、残高不足の旨のメッセージを電子マネー端末１５に送信する。電子マネー端末１５は、残高不足のため、指示された金額が移転できない旨のメッセージを表示する。

【０１４２】残高が指示された譲渡金額以上の場合、電子マネーサーバ１３は、電子マネーカード１９Ａの個人公開鍵Ｐk2Ａを用いて取引認証子｛Ｐk1Ａ（端末ＩＤ＋取引情報＋１９Ａのカードｉｄ）｝を端末ＩＤと取引情報と電子マネーカード１９Ａのカードｉｄとに変換する。又、電子マネーカード１９Ｂの個人公開鍵Ｐk2Ｂを用いて取引先認証子｛Ｐk1Ｂ（端末ＩＤ＋取引情報＋１９Ｂのカードｉｄ）｝を端末ＩＤと取引情報と電子マネーカード１９Ｂのカードｉｄとに変換する。次に、変換した内容が正しいか否かを判別する。即ち、取引認証子と取引先認証子から復号された取引情報及び端末ＩＤが一致しており、取引認証子から変換されたカードＩＤが譲渡元の電子マネーカード１９Ａのカードｉｄに一致し、取引先認証子から変換したカードＩＤが譲渡先の電子マネーカード１９Ｂのカードｉｄに一致することをチェックする。全て一致すると判別された場合、残高テーブルの電子マネーカード１９Ａと電子マネーカード１９Ｂの残高をそれぞれ更新する。

【０１４３】次に、電子マネーサーバ１３は、電子マネーカード１９Ａと電子マネーカード１９Ｂのカードｉｄ及び個人公開鍵を認証付与要求と共に認証局１１に送信する（Ｐ４４）。

【０１４４】認証局１１は、認証付与要求に応答し、受信した電子マネーカード１９Ａと１９Ｂのカードｉｄ及び個人公開鍵Ｐk2Ａ、Ｐk2Ｂを、自己が記憶するカードＩＤ及び個人公開鍵のリストに登録されているか否かをチェックする。これらが登録されていると判断された場合、それらに対してセンタ秘密鍵Ｃk1を用いて認証情報｛Ｃk1（１９Ａのカードｉｄ＋Ｐk2Ａ）｝、｛Ｃk1（１９Ｂのカードｉｄ＋Ｐk2Ｂ）｝をそれぞれ生成し、認証完了電文と共に電子マネーサーバ１３に送信する（Ｐ４５）。

【０１４５】電子マネーサーバ１３は、認証完了電文に応答し、譲渡元の電子マネーカード１９Ａの取引履歴と譲渡先の電子マネーカード１９Ｂの取引履歴を生成し記

憶する。さらに、それらの取引履歴に認証局１１からの認証情報を付加し、譲渡完了電文と共に電子マネー端末１５に送信する（Ｐ４６）。

【０１４６】電子マネー端末１５は、取引履歴と認証情報を受信すると、センター公開鍵Ck2を用いて認証情報をカードＩＤと個人公開鍵Pk2に変換し、チェックする。その認証情報が正しいものであると確認すると、譲渡完了電文に応答し、受信した取引履歴を電子マネーカード１９Ａと電子マネーカード１９Ｂへそれぞれ送信する（Ｐ４７）。電子マネーカード１９Ａと１９ＢのＩＣ部２０は、受信した取引履歴に基づいて、それぞれが記憶している残高を更新する。即ち、電子マネーカード１９ＡのＩＣ部２０は、受信した取引履歴に基づいて、記憶している残高を所定金額減額し、電子マネーカード１９ＢのＩＣ部２０は、受信した取引履歴に基づいて、記憶している残高を所定金額増額する。

【０１４７】さらに、電子マネーカード１９Ａ、１９ＢのＩＣ部２０は、それぞれ、最終取引ポインタの値を電子マネー端末１５に送信する。電子マネー端末１５は、電子マネーカード１９Ａと１９Ｂの光記憶部２１の、最終取引ポインタの値が示すアドレスの次のアドレスに受信した取引履歴を追記する。さらに、最終取引ポインタ及び送信済みポインタを、追記された取引履歴を示すように更新する。その後、電子マネー端末１５Ｃは、電子マネーの譲渡が完了した旨を表示部３２に表示すると共に電子マネーカード１９Ａと１９Ｂを排出する。

【０１４８】この電子マネー譲渡処理を、利用者Ａが電子マネーカード１９Ａ（カードＩＤ”Ｃ９９”）から電子マネーカード１９Ｂ（カードＩＤ”Ｃ０５”）へ、電子マネー端末１５Ｃ（端末ＩＤ”Ｔ１５０”）を介して３万円分の電子マネーを譲渡する場合を例に図１８を参照して説明する。

【０１４９】まず、利用者Ａは、図８に示す画面表示に従って、処理メニューから「3）電子マネーの譲渡」を選択し、電子マネーカード１９Ａを譲渡元カード挿入口３５Ａに挿入し、電子マネーカード１９Ｂを譲渡先カード挿入口３５Ｂに挿入し、譲渡金額を入力する。

【０１５０】この入力に応答して、電子マネー端末１５Ｃは、電子マネーカード１９Ａと電子マネーカード１９Ｂに、取引区分と利用年月日と取引金額とから構成される取引情報と端末ＩＤ”Ｔ１５０”と共に、カードＩＤと個人公開鍵の要求を示す要求信号をそれぞれ送信する（Ｌ４１）。

【０１５１】電子マネーカード１９Ａは、要求信号に応答し、端末ＩＤ”Ｔ１５０”と取引情報に自己のカードＩＤ”Ｃ９９”を加え、個人秘密鍵Pk1Aを用いて取引認証子｛Pk1A（Ｔ１５０＋取引情報＋Ｃ９９）｝を作成し、その取引認証子をカードＩＤ”Ｃ９９”と個人公開鍵Pk2Aと共に電子マネー端末１５Ｃに送信する（Ｌ４２）。

【０１５２】また、電子マネーカード１９Ｂは、要求信号に応答し、端末ＩＤ”Ｔ１５０”と取引情報に自己のカードＩＤ”Ｃ０５”を加え、個人秘密鍵Pk1Bを用いて取引先認証子｛Pk1B（Ｔ１５０＋取引情報＋Ｃ０５）｝を作成し、その取引先認証子をカードＩＤ”０５”と個人公開鍵Pk2Bと共に電子マネー端末１５Ｃに送信する（Ｌ４２）。

【０１５３】電子マネー端末１５Ｃは、電子マネーカード１９Ａから受信したカードＩＤ”Ｃ９９”と個人公開鍵Pk2Aと取引認証子｛Pk1A（Ｔ１５０＋取引情報＋Ｃ９９）｝と、電子マネーカード１９Ｂから受信したカードＩＤ”Ｃ０５”と個人公開鍵Pk2Bと取引先認証子｛Pk1B（Ｔ１５０＋取引情報＋Ｃ０５）｝と、電子マネーカード１９Ａから電子マネーカード１９Ｂへ３万円の電子マネーを移動するよう指示する譲渡依頼電文とを、電子マネーサーバ１３に送信する（Ｌ４３）。なお、譲渡依頼電文は端末ＩＤ”Ｔ１５０”を含む。

【０１５４】電子マネーサーバ１３は、受信した電子マネーカード１９Ａと電子マネーカード１９ＢのカードＩＤ”Ｃ９９”、”Ｃ０５”及び端末ＩＤ”Ｔ１５０”が事故カードＩＤ及び事故端末ＩＤのリストに登録されているか否かをチェックする。カードＩＤ”Ｃ９９”、”Ｃ０５”及び端末ＩＤ”Ｔ１５０”が、事故カード又は事故端末として登録されていないと判別された場合、電子マネーサーバ１３は、譲渡元の電子マネーカード１９Ａの残高を残高テーブルを参照してチェックする。

【０１５５】残高が３万円未満ならば、電子マネーサーバ１３は、残高不足の旨のメッセージを電子マネー端末１５に送信する。残高が３万円以上ならば、電子マネーサーバ１３は、個人公開鍵Pk2Aを用いて取引認証子｛Pk1A（Ｔ１５０＋取引情報＋Ｃ９９）｝を端末ＩＤと取引情報と電子マネーカード１９ＡのカードＩＤとに変換する。又、個人公開鍵Pk2Bを用いて取引先認証子｛Pk1B（Ｔ１５０＋取引情報＋Ｃ０５）｝を端末ＩＤと取引情報とカードＩＤとに変換する。

【０１５６】続いて、これらの内容が正しいか否かを判別する。即ち、取引認証子と取引先認証子から変換した端末ＩＤと取引情報とが互いに一致しており、取引認証子から変換されたカードＩＤが譲渡元の電子マネーカード１９ＡのカードＩＤ”Ｃ９９”に一致し、取引先認証子から変換されたカードＩＤが譲渡先の電子マネーカード１９ＢのカードＩＤ”Ｃ０５”に一致するか否かをチェックする。チェックの結果、取引認証子と取引先認証子が正しいと判別されたならば、電子マネーサーバ１３は、残高テーブルにおけるカードＩＤ”Ｃ９９”の残高を３万円だけ減算し、カードＩＤ”Ｃ０５”の残高に３万円を加算する。次に電子マネーサーバ１３は、電子マネーカード１９Ａと電子マネーカード１９ＢのカードＩＤ”Ｃ９９”、”Ｃ０５”及び個人公開鍵Pk2A、Pk2Bを認証局１１に認証付与要求と共に送信する（Ｌ４

４）。

【０１５７】認証局１１は、認証付与要求に応答し、自己が記憶するカードＩＤ及び公開鍵を参照することにより、受信した電子マネーカード１９Ａと電子マネーカード１９Ｂのカードｉｄ”Ｃ９９”、”Ｃ０５”及び個人公開鍵Ｐｋ2Ａ、Ｐｋ2Ｂがこのシステムに登録されているか否かをチェックする。認証局１１は、それらが登録されていることを確認すると、カードＩＤ”Ｃ９９”、”Ｃ０５”及び個人公開鍵Ｐｋ2Ａ、Ｐｋ2Ｂに対してセンタ秘密鍵Ｃｋ1を用いて電子マネーカード１９Ａの認証情報｛Ｃｋ1（Ｃ９９＋Ｐｋ2Ａ）｝と電子マネーカード１９Ｂの認証情報｛Ｃｋ1（Ｃ０５＋Ｐｋ2Ｂ）｝をそれぞれ生成し、認証完了電文と共に電子マネーサーバ１３に送信する（Ｌ４５）。

【０１５８】電子マネーサーバ１３は、電子マネーカード１９Ａと電子マネーカード１９Ｂの認証情報｛Ｃｋ1（Ｃ９９＋Ｐｋ2Ａ）｝と｛Ｃｋ1（Ｃ０５＋Ｐｋ2Ｂ）｝を受信すると、譲渡元の電子マネーカード１９Ａの取引履歴と譲渡先の電子マネーカード１９Ｂの取引履歴を生成し、取引履歴テーブルに記憶する。さらに、それらの取引履歴に認証局１１からの認証情報を付与し、譲渡完了電文と共に電子マネー端末１５Ｃに送信する（Ｌ４６）。

【０１５９】電子マネー端末１５は、取引履歴と認証情報を受信すると、センター公開鍵Ｃｋ2を用いて認証情報をカードＩＤと個人公開鍵Ｐｋ2に変換し、チェックする。その認証情報が正しいものであると確認すると、受信した取引履歴を電子マネーカード１９Ａと１９ＢのＩＣ部２０にそれぞれ送信する（Ｌ４７）。電子マネーカード１９Ａと１９ＢのＩＣ部２０は、受信した取引履歴に基づいて記憶回路に記憶している残高を更新する。即ち、電子マネーカード１９Ａは残高を３万円減額し、電子マネーカード１９Ｂは残高を３万円増額する。さらに、電子マネー端末１５Ｃは、電子マネーカード１９Ａと１９ＢのＩＣ部２０から最終取引ポインタの値を読み出し、電子マネーカード１９Ａと１９Ｂの光記憶部２１の最終取引ポインタが値が示すアドレスの次のアドレスに、取引履歴をそれぞれ追記する。

【０１６０】さらに、端末１５Ｃは、電子マネーカード１９Ａと１９ＢのＩＣ部２０に記憶されている最終取引ポインタ及び送信済みポインタを追記された取引履歴を示すように更新する。その後、電子マネー端末１５Ｃは、電子マネーの譲渡が完了した旨を表示部３２に表示すると共に電子マネーカード１９Ａと１９Ｂを排出する。

【０１６１】なお、譲渡元の電子マネーカード１９Ａの残高のチェックは、「３）電子マネーの譲渡」がメニューより選択され、譲渡金額が入力されたときに電子マネー端末１５が行うようにしてもよい。この場合、電子マネー端末１５は、電子マネーカード１９Ａに残高要求を

行う。

【０１６２】以上の説明では、電子マネーの譲渡処理をオンライン処理により実行したが、譲渡額が一定額以下の場合は、電子マネー支払処理と同様、電子マネー端末１５内で処理するオフライン方式にしてもよい。これにより、レスポンス速度を向上することができる。オフライン処理の場合、セキュリティを高めるため、１回の譲渡金額の限度を定めてもよい。

【０１６３】（６）電子マネー換金処理

次に、電子マネーカード１９に蓄積している電子マネーを換金し、利用者の決済口座に振り込む電子マネー換金処理の概要を図１９を参照して説明する。まず、利用者は、図８に示すように、表示部３２に表示される処理メニューから「２）電子マネーの換金」を選択し、電子マネーカード1.9を電子マネー端末１５に挿入し、換金金額を入力する。

【０１６４】電子マネー端末１５は、この選択に応答し、取引区分と利用年月日と取引金額とから構成される取引情報と端末ＩＤと、カードＩＤと個人公開鍵の要求を示す要求信号とを、電子マネーカード１９に送信する（Ｐ５１）。

【０１６５】電子マネーカード１９は、要求信号に応答し、端末ＩＤと取引情報に自己のカードＩＤを加え、個人秘密鍵Ｐｋ1を用いて取引認証子｛Ｐｋ1（端末ＩＤ＋取引情報＋カードＩＤ）｝を作成し、作成した取引認証子をカードＩＤと個人公開鍵と共に電子マネー端末１５に送信する（Ｐ５２）。

【０１６６】電子マネー端末１５は、受信したカードＩＤに取引情報と端末ＩＤを加え、端末秘密鍵Ｔｋ1を用いて取引先認証子｛Ｔｋ1（端末ＩＤ＋取引情報＋カードＩＤ）｝を作成する。電子マネー端末１５は、作成した取引先認証子｛Ｔｋ1（端末ＩＤ＋取引情報＋カードＩＤ）｝と、入力された換金金額と、電子マネーカード１９から対応する決済口座に振り換えることを指示し、端末公開鍵Ｔｋ2を含む換金要求と、電子マネーカード１９のカードＩＤと、個人公開鍵Ｐｋ2とを電子マネーサーバ１３に送信する（Ｐ５３）。なお、チャージ要求電文は、送信元の電子マネー端末１５の端末ＩＤを含む。

【０１６７】電子マネーサーバ１３は、受信した電子マネーカード１９のカードＩＤ及び端末ＩＤを自己が記憶する事故カードＩＤリスト及び事故端末ＩＤのリストに登録されているか否かをチェックする。受信したカードＩＤ及び端末ＩＤが、事故カードＩＤリスト及び事故端末ＩＤリストに登録されていないと判別された場合、電子マネーサーバ１３は、受信した個人公開鍵Ｐｋ2を用いて取引認証子｛Ｐｋ1（端末ＩＤ＋取引情報＋カードＩＤ）｝を端末ＩＤと取引情報とカードＩＤとに変換する。又、受信した端末公開鍵Ｔｋ2を用いて取引先認証子｛Ｔｋ1（端末ＩＤ＋取引情報＋カードＩＤ）｝を端末ＩＤと取引情報とカードＩＤとに変換し、これらが一致す

るか否かを判別する。これらが一致した場合、電子マネーサーバ１３は、取引認証子｛Ｐk1（端末ＩＤ＋取引情報＋カードＩＤ）｝と取引先認証子｛Ｔk1（端末ＩＤ＋取引情報＋カードＩＤ）｝は正しいと判別し、カードＩＤ及び個人公開鍵Ｐk2を認証付与要求と共に認証局１１に送信する（Ｐ５４）。

【０１６８】認証局１１は、認証付与要求に応答し、自己が記憶しているカードＩＤ及び個人公開鍵のリストを参照することにより、受信したカードＩＤと個人公開鍵Ｐk2がシステムに登録されているかをチェックする。それらが登録されているならば、認証局１１は、センタ秘密鍵Ck1を用いて、受信したカードＩＤ及び個人公開鍵Ｐk2に対する認証情報｛Ck1（カードＩＤ＋Ｐk2）｝を生成し、電子マネーサーバ１３に送信する（Ｐ５５）。受信したカードＩＤ及び個人公開鍵Ｐk2がシステムに登録されていないならば、認証局１１は不正検出を電子マネーサーバ１３に通知する。

【０１６９】電子マネーサーバ１３は、認証局１１から認証情報｛Ck1（カードＩＤ＋Ｐk2）｝を受信すると、残高テーブルを参照して電子マネーカード１９Ａの残高をチェックし、振替可能であれば、カードＩＤと振替金額を含む振替依頼電文を作成し、銀行センタ１７に送信する（Ｐ５６）。

【０１７０】なお、受信したカードＩＤと端末ＩＤの少なくとも一方が使用不可のカードＩＤ及び端末ＩＤのリストのいずれかと一致する場合、又は取引認証子と取引先認証子から変換された端末ＩＤと取引情報とカードＩＤとが互いに一致しない場合、電子マネーサーバ１３は、電子マネー端末１５にチャージ不可の旨のメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者に通知する。また、電子マネーカード１９の残高が不足している場合は、電子マネーサーバ１３は、残高不足の旨のメッセージを電子マネー端末１５に送信する。

【０１７１】銀行センタ１７は、振替依頼電文を受信すると、図５に示す口座テーブルを参照して、指示された金額を別段口座からカードＩＤに対応する決済口座に振り替える（Ｐ５７）。振り替え完了後、銀行センタ１７は、振替完了電文を電子マネーサーバ１３に送信する（Ｐ５８）。

【０１７２】電子マネーサーバ１３は、振替完了電文を受信すると、電子マネーカード１９の残高テーブルの残高を更新し、取引履歴を生成し、取引履歴テーブルに記憶する。次に電子マネーサーバ１３は、認証局１１からの認証情報｛Ck1（カードＩＤ＋Ｐk2）｝を取引履歴に付与し、換金が完了したことを示す換金完了電文と共に電子マネー端末１５に送信する（Ｐ５９）。

【０１７３】電子マネー端末１５は、取引履歴と認証情報｛Ck1（カードＩＤ＋Ｐk2）｝と振替完了電文とを受信すると、センター公開鍵Ck2を用いて認証情報｛Ck1

（カードＩＤ＋Ｐk2）｝をカードＩＤと個人公開鍵Ｐk2に変換し、チェックする。その認証情報が正しいものであると確認すると、電子マネーカード１９に取引履歴を送信する（Ｐ６０）。

【０１７４】電子マネーカード１９のＩＣカード部２０は、受信した取引履歴に基づいて、残高を更新すると共に最終取引ポインタの値を電子マネー端末１５に送信する。電子マネー端末１５は、受信した取引履歴を光記憶部２１の最終取引ポインタが指示するアドレスの次のアドレスに追記する。続いて、ＩＣカード部２０に記憶されている最終取引ポインタと送信済みポインタを更新する。その後、電子マネー端末１５は、電子マネーの換金が完了した旨を表示部３２に表示すると共に電子マネーカード１９を排出する。

【０１７５】この電子マネー換金処理を、利用者Ａが電子マネーカード１９Ａ（カードＩＤ”Ｃ９９”）に記憶している電子マネーのうち５万円を、電子マネー端末１５Ｂ（端末ＩＤ”Ｔ１５０”）を用いて、銀行センタ１７の自己の決済口座に振り替える場合を例に図２０を参照して説明する。利用者Ａは、表示部３２に表示される処理メニューから「2）電子マネーの換金」を選択し、電子マネーカード１９Ａを電子マネー端末１５Ｂに装着し、換金金額「５万円」を入力部３１に入力する。

【０１７６】この操作に応答して、電子マネー端末１５Ｂは、電子マネーカード１９Ａに、取引区分と利用年月日と取引金額とから構成される取引情報と、端末ＩＤ”Ｔ１５０”と、カードＩＤと個人公開鍵の送信を要求する要求信号と、を送信する（Ｌ５１）。電子マネーカード１９Ａは、要求信号に応答し、受信した端末ＩＤ”Ｔ１５０”及び取引情報に自己のカードＩＤ”Ｃ９９”を加え、個人秘密鍵Ｐk1Ａを用いて取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝を作成する。電子マネーカード１９Ａは、作成した取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝とカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを電子マネー端末１５Ｂに送信する（Ｌ５２）。

【０１７７】電子マネー端末１５Ｂは、受信したカードＩＤ”Ｃ９９”に取引情報と端末ＩＤ”Ｔ１５０”を加え、端末秘密鍵Tk1を用いて取引先認証子｛Tk1Ｂ（Ｔ１５０”＋取引情報＋Ｃ９９）｝を作成する。電子マネー端末１５Ｂは、作成した取引先認証子｛Tk1Ｂ（Ｔ１５０”＋取引情報＋Ｃ９９）｝と、入力された換金金額を電子マネーカード１９Ａからその電子マネーカード１９Ａに対応する決済口座に振り換えることを指示し、端末公開鍵Tk2Ｂを含む換金要求と、電子マネーカード１９ＡのカードＩＤ”Ｃ９９”と、個人公開鍵Ｐk2Ａと、取引認証子｛Ｐk1Ａ（Ｔ１５０”＋取引情報＋Ｃ９９）｝とを電子マネーサーバ１３へ送信する（Ｌ５３）。

【０１７８】電子マネーサーバ１３は、電子マネーカー

ド１９ＡのカードＩＤ”Ｃ９９”及び端末ＩＤ”Ｔ１５０”が事故カードＩＤリスト及び事故端末ＩＤリストに登録されているか否かチェックする。受信したカードＩＤ”Ｃ９９”及び端末ＩＤ”Ｔ１５０”が、事故カードＩＤリスト及び事故端末ＩＤリストに登録されていないと判別された場合、電子マネーサーバ１３は、受信した個人公開鍵Ｐk2Ａを用いて取引認証子｛Ｐk1Ａ（Ｔ１５０”＋取引情報＋Ｃ９９）｝を取引情報とカードＩＤと端末ＩＤに変換する。さらに、受信した端末公開鍵Ｔk2Ｂを用いて取引先認証子｛Ｔk1Ｂ（Ｔ１５０”＋取引情報＋Ｃ９９）｝を取引情報とカードＩＤと端末ＩＤに変換し、これらが相互に一致するか否かを判別する。一致した場合、電子マネーサーバ１３は、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを認証付与要求と共に認証局１１に送信する（Ｌ５４）。

【０１７９】認証局１１は、自己が記憶しているカードＩＤ及び個人公開鍵を参照し、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａがシステムに登録されているかをチェックし、登録済みであることを確認すると、センタ公開鍵Ｃk1を用いて認証情報｛Ｃk1（Ｃ９９＋Ｐk2Ａ）｝を生成し、認証完了電文と共に電子マネーサーバ１３に送信する（Ｌ５５）。電子マネーサーバ１３は、認証局１１から認証完了電文と認証情報｛Ｃk1（Ｃ９９＋Ｐk2Ａ）｝を受信すると、残高テーブルのカードＩＤ”Ｃ９９”の残高が換金金額の５万円以上か否かを判別する。残高が５万円以上ならば、電子マネーサーバ１３は、銀行センタ１７へカードＩＤ”Ｃ９９”と振替金額”５万円”を含む振替依頼電文を送信する（Ｌ５６）。

【０１８０】銀行センタ１７は、電子マネーサーバ１３から振替依頼電文を受信すると、口座テーブルを参照し、別段口座からカードＩＤ”Ｃ９９”に対応する利用者Ａの決済口座に５万円を振り替える。振替処理が完了すると、銀行センタ１７は振替完了電文を電子マネーサーバ１３に送信する（Ｌ５７）。電子マネーサーバ１３は、振替完了電文を受信すると、残高テーブルのカードＩＤ”Ｃ９９”の残高から５万円を減算し、取引履歴を生成し、取引履歴テーブルに記憶する。次に、電子マネーサーバ１３は、認証局１１からの認証情報｛Ｃk1（Ｃ９９＋Ｐk2Ａ）｝を取引履歴に付与し、換金完了電文と共に電子マネー端末１５Ｂに送信する（Ｌ５８）。

【０１８１】電子マネー端末１５Ｂは、換金完了電文に応答し、センター公開鍵Ｃk2を用いて認証情報｛Ｃk1（Ｃ９９＋Ｐk2Ａ）｝をカードＣ９９と個人公開鍵Ｐk2に変換し、チェックする。その認証情報が正しいものであると確認すると、取引履歴を電子マネーカード１９Ａに送信する（Ｌ５９）。電子マネーカード１９ＡのＩＣ部２０は、受信した取引履歴に基づいて、自己が記憶する残高から５万円を減算する。さらに、電子マネー端末１５Ｂは、受信した取引履歴を光記憶部２１の最終取引

ポインタが指示する位置に追記し、最終取引ポインタと及び送信済みポインタの値を更新する。その後、電子マネー端末１５Ｂは、電子マネーの換金が完了した旨を表示部３２に表示すると共に電子マネーカード１９Ａを排出する。

【０１８２】このようにして、利用者は自己の電子マネーカード１９に蓄積している電子マネーを換金し、自己の決済口座に振り込むことができる。

【０１８３】以上説明したように、この電子マネーシステムにより、電子マネーを電子マネーカードにチャージし、換金し、譲渡し、支払いに使用することができる。しかも、光記憶部２１に取引履歴を記録するので、この追記型記憶部の記録内容を検証（追尾）することにより、不正行為等を容易に検出することができる。さらに、センタにおいても取引履歴を記録することにより、不正行為をより確実に検出することができる。

【０１８４】なお、この発明は上記実施の形態に限定されず、種々の変形及び応用が可能である。例えば、取引履歴の構成要素は任意であり、各取引に一意な取引ＩＤ、その時点での電子マネーの残高、取引時分秒等を取引履歴に含めても良い。また、認証情報等を取引履歴から削除してもよい。

【０１８５】光記憶部２１に記録する取引履歴からそのカードを特定する情報を省略してもよい。例えば、電子マネーカード１９Ａに電子マネーをチャージした場合、電子マネーカード１９Ａの光記憶部２１には、例えば、取引がチャージであること、取引日時、取引金額、端末ＩＤ等を記録し、自己を特定する情報は記録する必要がない。

【０１８６】同様に、例えば、電子マネーカード１９Ａから電子マネーカード１９Ｂに電子マネーを移動した場合に、電子マネーカード１９Ａの光記憶部２１には、取引区分が電子マネーの譲渡であること、譲渡先の電子マネーカード１９ＢのカードＩＤ、移転金額等を記録し、移転元（電子マネーカード１９Ａ）を特定する情報を記録せず、電子マネーカード１９Ｂの光記憶部２１には、電子マネーの譲受であること、譲渡元の電子マネーカード１９ＡのカードＩＤ、移転金額等を記録し、移転先（電子マネーカード１９Ｂ）を特定する情報を記録しないように構成してもよい。これにより、光記憶部２１の記録データの量を削減できる。

【０１８７】上記実施の形態では、電子マネーカードの利用者の決済口座のリストを銀行センタ１７に登録し、カードＩＤを決済口座の口座番号に変換したが、決済口座の口座番号を電子マネーカード１９のＩＣ部２０又は光記憶部２１に登録しておき、電子マネーのチャージ、換金等の処理を行う際に、電子マネーカード１９から口座番号を銀行センタ１７に通知してもよい。

【０１８８】上記実施の形態では、個人認証情報を生成、確認するために署名鍵Ｓkと検査鍵Ｅkを用いたが、

センタ秘密鍵Ｃk1とセンタ公開鍵Ｃk2を用いてもよい。

【０１８９】ワイドエリアのネットワーク（例えば、インターネット等）のネットワーク上でこの電子マネーシステムを構築する場合は、認証局１１と電子マネーサーバ１３をそれぞれ設けることが望ましいが、クローズドループ型のローカルネットワークでは、認証局１１と電子マネーサーバ１３を、１つのサーバとして実現してもよい。

【０１９０】また、この電子マネーシステムを、図２１に示すように、認証局１１を除いた構成にしてもよい。この場合の、各処理の概要を図２２～図２６に示す。この場合の処理は、図２２～図２６と従前の図面を参照すれば明らかなように、センタ秘密鍵及びセンタ公開鍵、個人秘密鍵及び個人公開鍵、認証に関する処理がなくなった点をを除けば、実施の形態の動作と同一である。この構成によれば、システム全体において処理速度が向上する。

【０１９１】また、システムのセキュリテイを高めるため、例えば、電子マネー端末１５の操作者の正当性を操作者の身体的特徴に基づいて判別してもよい。例えば、電子マネーカード１９のＩＣ部２０の記憶回路に所持者の指紋データを配置しておき、電子マネー端末１５の操作者の指紋をスキャンし、これらが一致する場合にのみ、以後の電子マネー取引処理を実行しても良い。

【０１９２】この場合、電子マネー端末１５には、図２７に示すような指紋読取装置４１が接続される。指紋読取装置４１は、指紋をスキャンするための読取窓４１Ａと指を案内するためのガイド４１Ｂを備える。また、ＩＣ部２０の記憶回路には、図２８に示すように、保持者の指紋の画像をフーリエ変換した後、抽出された位相情報が予め登録されている。

【０１９３】指紋読取装置４１は、図２８に示すように、読取窓４１Ａ内の画像（指紋の画像）をスキャンし、画像データを取得する画像取得部５１と、画像取得部５１で取得した画像データ（の波形）をフーリエ変換するフーリエ変換部５２と、フーリエ変換部５２で取得されたフーリエ級数の位相情報のみを抽出する位相情報抽出部５３と、ＩＣ部２０から読み出した位相情報と位相情報抽出部５３で生成された位相情報を合成する位相合成部５４と、合成部５４で合成された位相情報をフーリエ変換して相関強度を得るフーリエ変換部５５と、フーリエ変換部５５で得られた相関強度と閾値を比較し、操作者が正当者であるか否かを判別する判別部５６とより構成される。

【０１９４】このような構成において、例えば、処理メニューの中から処理を選択し、電子マネーカード１９を挿入すると、電子マネー端末１５は、図２９に示すように、指紋読取装置４１上に指を置く旨のメッセージを表示する。操作者がメッセージに従って指紋読取装置４１上に指を置くと、指紋読取装置４１の画像取得部５１は、読取窓４１Ａ内の指紋をスキャンし、その画像を取り込む。フーリエ変換部５２は、読み取られた画像をフーリエ変換し、位相情報抽出部５３が位相情報を取り込む。

【０１９５】続いて、位相合成部５４は、ＩＣ部２０に登録されている位相情報を読み出し、位相情報抽出部５３から抽出された位相情報と合成し、さらに、フーリエ変換部５５は合成データをフーリエ変換し、相関強度を求める。

【０１９６】判定部５６は、相関強度が一定値以上の場合に、予めＩＣ部２０に登録されている指紋と読み取った指紋が類似し、操作者が電子マネーカード１９の正当な保持者であると判別し、選択した処理に対応する以後の処理を可能とするように制御する。相関強度が一定値未満の場合、予めＩＣ部２０に登録されている指紋と読み取った指紋が類似しないと判断し、表示部３２に指紋照合が一致しないため、以後の操作ができない旨を表示し、電子マネーカード１９を排出する。

【０１９７】このような構成によれば、操作者の身体的特徴に基づいて、操作者が正当な者か否かを判別し、電子マネーの取引を許可するか否かを判別することができる。従って、電子マネーの不正使用を有効に防止できる。

【０１９８】なお、指紋の類似度を判別する手法及び回路は図２８に示す回路及び方法に限定されず、他の手法を使用してもよい。また、身体的特徴としては、指紋に限らず、声紋、顔のパターン、網膜パターン等を使用してもよい。声紋を使用する場合には、声紋の特徴データをＩＣ部２０に格納し、電子マネー端末１５にマイクロフォンを配置し、マイクロフォンで取得した音声の特徴データを抽出し、ＩＣ部２０に格納しておいた特徴データとの相関強度を判別し、相関強度が一定値以上の場合に操作者が正当者であると判別する。

【０１９９】また、顔のパターン、網膜パターン等を使用する場合には、顔、網膜パターンの特徴データをＩＣ部２０に格納し、電子マネー端末１５にカメラを配置し、カメラで取得した、画像の特徴データを抽出し、ＩＣ部２０に格納しておいた特徴データとの相関強度を判別し、相関強度が一定値以上の場合に操作者が正当者であると判別する。

【０２００】なお、予め抽出された特徴データは、ＩＣ部２０に格納されてもよく、光記憶部２１に格納されても良い。また、取引の際に使用した身体的特徴を示す特徴データを光記憶部２１に取引履歴情報の一部として記録してもよい。

【０２０１】電子マネーを扱うシステムでは、例えば、利用者のカードＩＤ等の情報を入手して、そのカードＩＤの所有者になりすまして認証を得ようとする不正行為が考えられる。このような不正行為を防ぐために、通信電文等を例えばＲＳＡ方式等の暗号方式を用いて暗号化

することにより、そのセキュリテイを高めることができる。

【０２０２】この場合、例えば、認証局１１は、センタ秘密鍵Ck1とセンタ公開鍵Ck2を生成し、記憶する。認証局１１は、電子マネーサーバ１３にセンタ秘密鍵Ck1をコピーすることにより、センタ秘密鍵Ck1をセンタ１０内で共有化する。また、認証局１１は、センタ公開鍵Ck2を各電子マネー端末１５及び電子マネーカード１９等に電子マネーサーバ１３を介して予め配布する。

【０２０３】各電子マネーカード１９及び電子マネー端末１５は、センタ公開鍵Ck2を用いて各々の情報（電子マネーカード１９ならばカードＩＤ及び個人公開鍵、電子マネー端末１５ならばチャージ要求、種々の電文等）を暗号化し、電子マネーサーバ１３に送信する。電子マネーサーバ１３がセンタ秘密鍵Ck1を用いてそれらの情報を復号化し、処理する。電子マネーサーバ１３は、電子マネーカード１９から送られてきた個人公開鍵を用いて取引履歴を暗号化し、電子マネー端末１５を介して電子マネーカード１９に送信する。

【０２０４】このような手法を用いることにより、電子マネーカード１９及び電子マネー端末１５からの情報は、センタ１０内の電子マネーサーバ１３及び認証局１１しか復号化することができず、又、電子マネーサーバ１３からの取引履歴は、電子マネー端末１５で参照されることなく、電子マネーカード１９に送信され、復号化される。更に、秘密鍵・公開鍵を定期的に変更することにより、よりセキュリティを高めることができる。

【０２０５】なお、認証局１１は、センタ秘密鍵Ck1及び公開鍵Ck2を定期的又は不定期に変更し、センタ公開鍵Ck2を電子マネー端末１５へ、センタ秘密鍵Ck1を電子マネーサーバ１３へ、それぞれ送信する。センタ秘密鍵Ck1及びセンタ公開鍵Ck2を変更した後、電子マネー端末１５に電子マネーカード１９が挿入されたとき、電子マネー端末１５は、新たなセンタ公開鍵Ck2を電子マネーカード１９に通知する。

【０２０６】また、暗号化の方式は、公開鍵方式に限定されず、共通鍵方式を用いてもよい。この場合、セキュリティの面から電子マネーカード１９の耐タンパー性を強化することが望ましい。

【０２０７】また、このシステムで取引が行われる度に、新たな暗号化のキー（秘密鍵と公開鍵の対、共通鍵等）を発行し、電子マネーカードに通知して、通知されたキーを用いて暗号化・復号化を行ってもよい。

【０２０８】さらに、キーを乱数に基づいて発生してもよい。このようなシステムによれば、次に発行されるキーの予測がつかず、情報の漏洩を防止できる。過去に発行されたキーと新たに発行されたキーを組み合わせて暗号化及び復号化用のキーとして使用してもよい。例えば、今回のキーK_tと前回のキーK_{t-1}　を組み合わせて$\{K_t + K_{t-1}\}$をキーとして用いて各種情報を暗号化し、さらに、復号化してもよい。

【０２０９】電子マネーシステムにおいては、電子マネーカード１９自体の完全なコピーを作成し、不正使用することが考えられる。この種の不正使用を防止するためには、電子マネーサーバ１３で、取引毎に固有の番号を電子マネーカード１９に付与し、オンライン取引開始時に、電子マネーカード１９からこの固有番号を電子マネーサーバ１３に送信し、電子マネーサーバに登録されているその電子マネーカード１９の固有番号に一致することを確認してから取引を行い、取引終了時等に、新たな固有番号を発生して電子マネーカード１９と電子マネーサーバ１３に登録するように構成すればよい。この構成によれば、取引の度に、固有番号が更新されるため、電子マネーカード１９のコピーを作成しても、１回取引を行うと、使用した１枚以外は固有番号が電子マネーサーバ１３に登録されているものと異なってしまうため、使用できなくなる。従って、電子マネーカード１９のコピーによる不正使用を防止できる。

【０２１０】なお、上記説明では、カードへの電子マネーのチャージ処理に際して、チャージ金額相当の現金を利用者の口座からシステムの決済口座に移動させて、該チャージ金額を支払うようにしているが、例えばクレジット（信用供与）による支払としてもよい。この場合、例えば、サーバが、チャージ要求の受信に応じて、該要求が示すチャージ金額、利用者の口座等の情報を貸付情報として一定期間記憶しておき、所定のタイミングで、利用者の口座から引き落とす。また、信用供与専用の口座を用意しておき、サーバが、チャージ要求の受信に応じて、該要求が示すチャージ金額をその口座から引き出す。ようにしてもよい。この場合は、入金があると、その利用者の貸し付け口座に入金金額を振り込む。クレジット、或いは貸し付けなどにより、電子マネーを発行する場合には、信用供与額及び／又は貸付可能残高（残枠）等が発行を要求された額より多いことを確認することが望ましい。その他、電子マネーの発行の経済的根拠自体は、任意である。

【０２１１】なお、この発明の電子マネー端末は、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、コンピュータに上述の動作を実行するためのプログラムを格納した媒体（フロッピーディスク、ＣＤ－ＲＯＭ等）から該プログラムをインストールすることにより、上述の処理を実行する電子マネー端末を構成することができる。

【０２１２】また、コンピュータにプログラムを供給するための媒体は、通信媒体（通信回線、通信ネットワーク、通信システムのように、一時的に且つ流動的にプログラムを保持する媒体）でも良い。例えば、通信ネットワークの掲示板（ＢＢＳ）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、ＯＳの制御下で、他のアプリケ

ーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【０２１３】

【発明の効果】以上説明したように、本発明によれば、電子マネーカードに電子マネーをチャージし、チャージした電子マネーを用いて種々の取引を行うことができる。しかも、追記型記憶部に取引履歴を記録するので、異常が発生した場合に、この追記型記憶部の記録内容を検証することにより、不正行為等を容易に検出することができる。さらに、センタにおいても取引履歴を記録することにより、不正行為をより確実に検出することができる。また、電子マネーを取引する際に、操作者の身体的特徴に基づいてその正当性を判別することにより、取引の信頼性を高めることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る電子マネーシステムの構成を示す図である。

【図２】（Ａ）は、電子マネーサーバが記憶している残高テーブルの構造を示す図、（Ｂ）は、電子マネーサーバが記憶している事故カードリストの構造を示す図、（Ｃ）は、電子マネーサーバが記憶している事故端末リストの構造を示す図である。

【図３】電子マネーサーバが記憶している取引履歴テーブルの構造を示す図である。

【図４】（Ａ）と（Ｂ）は、電子マネー端末の外観構成の例を示す図である。

【図５】銀行センタが記憶している口座テーブルの構造を示す図である。

【図６】電子マネーカードの構造を示す図である。

【図７】電子マネーチャージ処理の概要を示す図である。

【図８】（Ａ）～（Ｃ）は、電子マネー端末の表示例を示す図である。

【図９】電子マネーチャージ処理の流れを説明するための図である。

【図１０】個人認証情報発行処理の概要を示す図である。

【図１１】個人認証情報発行処理の流れを説明するための図である。

【図１２】電子マネー支払い処理の概要を示す図である。

【図１３】電子マネー支払い処理の流れを説明するための図である。

【図１４】突き合わせ処理の概要を示す図である。

【図１５】突き合わせ処理の流れを説明するための図である。

【図１６】突き合わせ処理において未送信履歴の送信前と送信後のＩＣ部と光記憶部と残高テーブルの状態を示す図である。

【図１７】電子マネー譲渡処理の概要を示す図である。

【図１８】電子マネー譲渡処理の流れを説明するための図である。

【図１９】電子マネー換金処理の概要を示す図である。

【図２０】電子マネー換金処理の流れを説明するための図である。

【図２１】認証局を含まない場合の電子マネーシステムの構成の一例を示す図である。

【図２２】認証局を含まない場合の電子マネーチャージ処理の流れを示す図である。

【図２３】認証局を含まない場合の電子マネー支払処理の流れを示す図である。

【図２４】認証局を含まない場合の突き合わせ処理の流れを示す図である。

【図２５】認証局を含まない場合の電子マネー譲渡処理の流れを示す図である。

【図２６】認証局を含まない場合の電子マネー換金処理の流れを示す図である。

【図２７】指紋読取装置の例を示す図である。

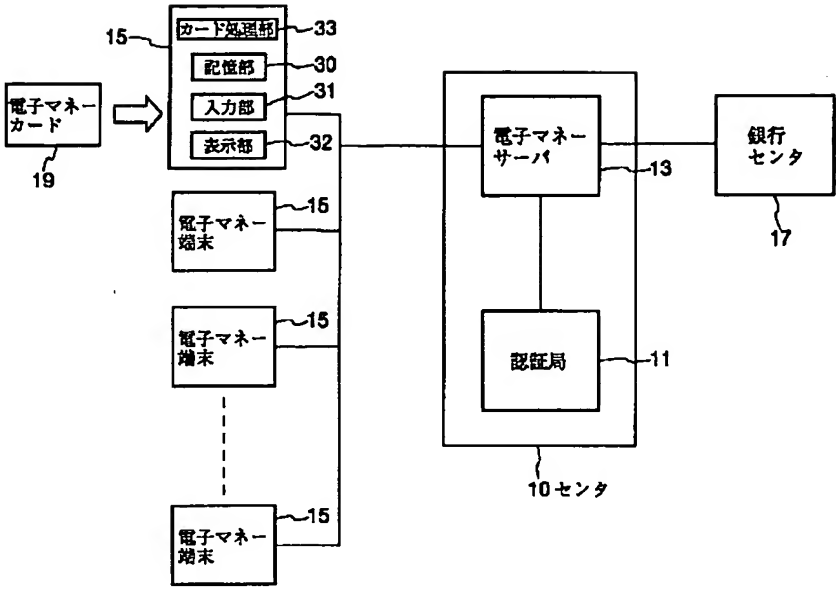
【図２８】指紋照合回路の構成例を示す図である。

【図２９】指紋照合時の電子マネー端末の表示例を示す図である。

【符号の説明】

１０　センタ
１１　認証局
１３　電子マネーサーバ
１５　電子マネー端末
１９　電子マネーカード
２０　ＩＣ部
２１　光記憶部
３０　記憶部
３１　入力部
３２　表示部
３３　カード処理部
３４　タッチパネル
３５、３５Ａ、３５Ｂ　カード挿入口
３６　金銭ドロア

【図１】



【図５】

口座テーブル

カードＩＤ	口座番号
C01	10002221
C03	12341234
C05	53334442
⋮	⋮
C99	30000001
⋮	⋮

【図２】

（Ａ）残高テーブル

カードＩＤ	残 高
C001	50000
C003	10000
C005	5000
C019	30000
⋮	⋮

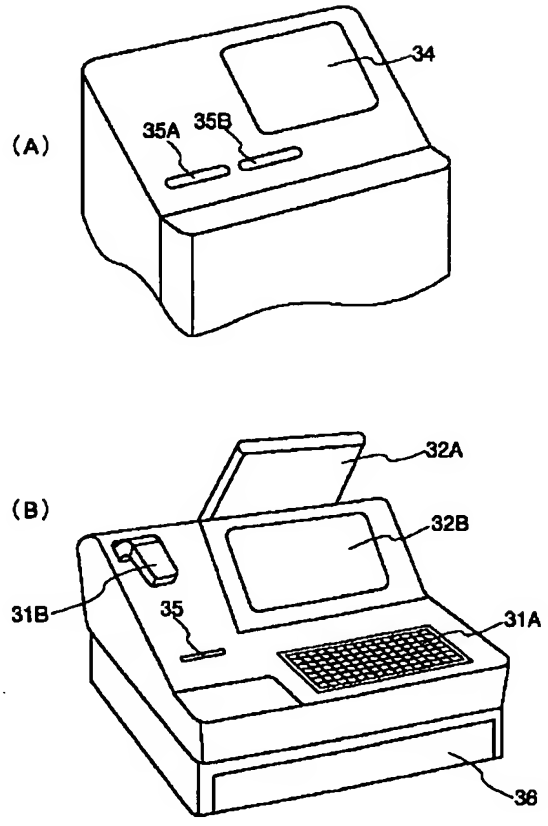
（Ｂ）事故カードリスト
（使用不可の電子マネーカードのカードＩＤリスト）

カードＩＤ（使用不可）
C010
C021
C033
C048
⋮

（Ｃ）事故端末リスト
（使用不可の電子マネー端末の端末ＩＤのリスト）

端末ＩＤ
T145
T247
T255
T301
⋮

【図４】



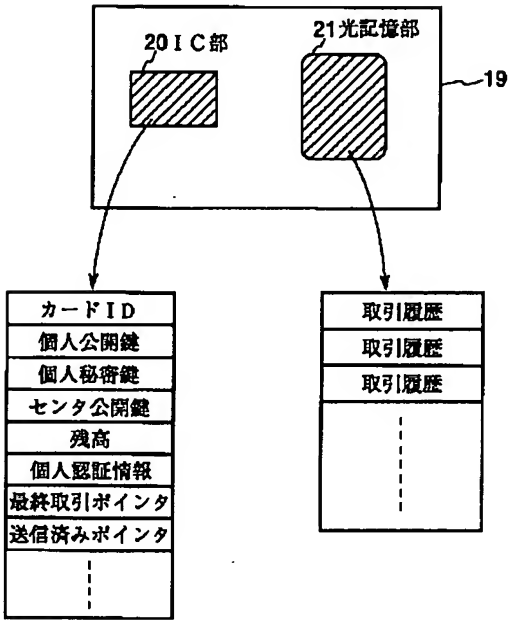
【図３】

取引履歴テーブル
カードＩＤ：ＣＸＸＸ

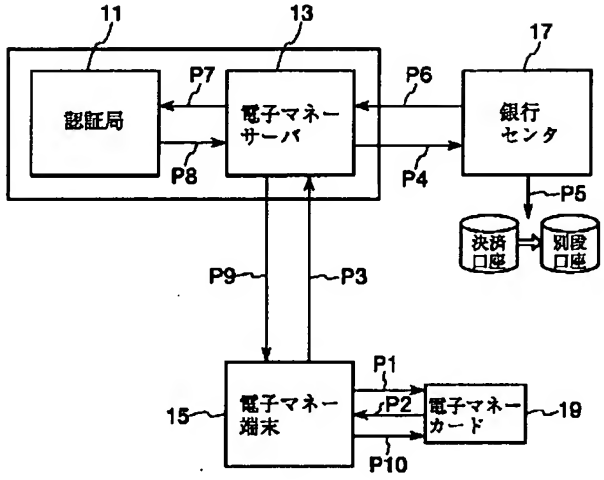
利用区分	利用年月日	取引金額	端末ＩＤ	取引先のカードＩＤ又は端末ＩＤ	認証子	
					取引認証子	取引先認証子
チャージ	1996/02/20	30000	T111	T111	XXXXXXXXX	XXXXXXXXX
購買	1996/04/15	50000	T126	C099	XXXXXXXXX	XXXXXXXXX
支払	1996/05/18	45000	T288	T288	XXXXXXXXX	XXXXXXXXX
現金	1996/06/25	10000	T451	T451	XXXXXXXXX	XXXXXXXXX
・	・	・	・	・	・	・
・	・	・	・	・	・	・
・	・	・	・	・	・	・
・	・	・	・	・	・	・
・	・	・	・	・	・	・
・	・	・	・	・	・	・

取引情報

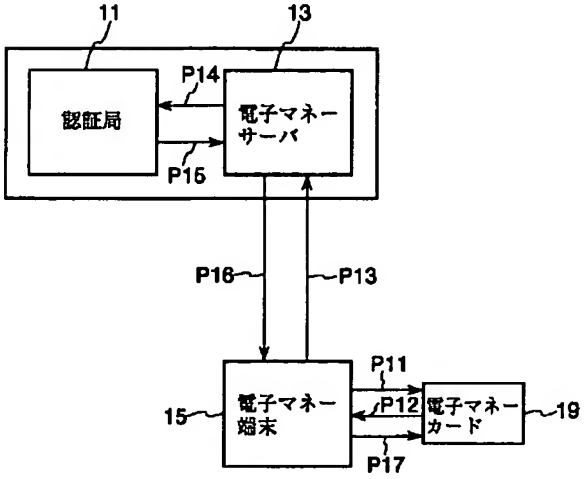
【図６】



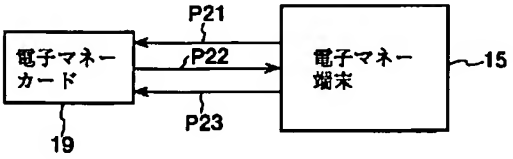
【図７】



【図１０】



【図１２】



【図８】

(A)

処理を選択してください

1）　電子マネーのチャージ
2）　電子マネーの換金
3）　電子マネーの譲渡
4）　個人認証情報の発行

～３２

(B)

電子マネーカードを
カード挿入口に挿入して
ください

～３２

(C)

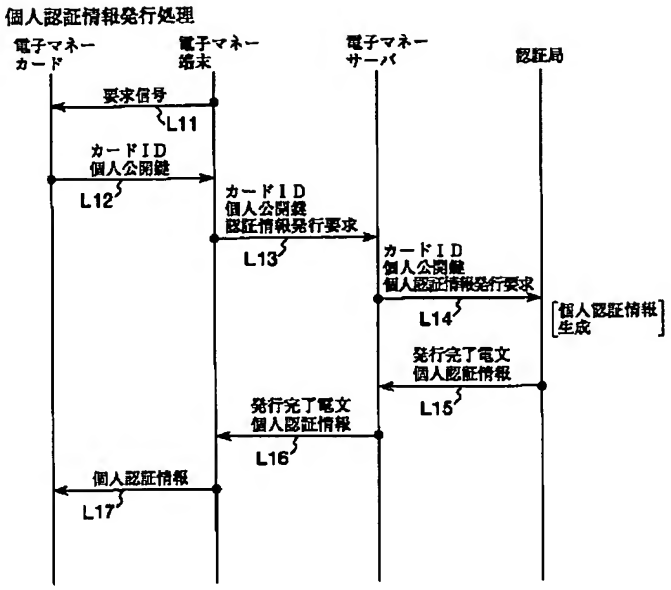
金額を入力してください

¥＿＿＿＿＿

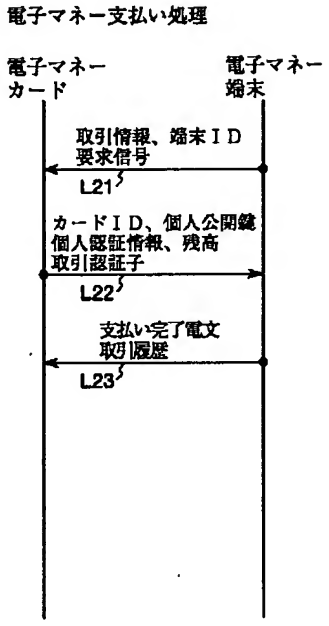
1　2　3　千　　確認
4　5　6　万　　訂正
7　8　9　0　円

～３２

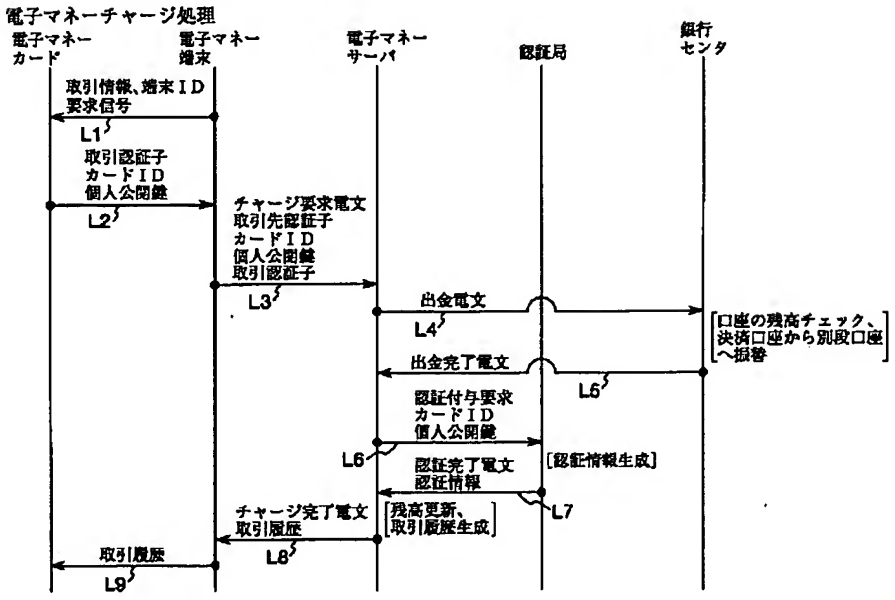
【図１１】



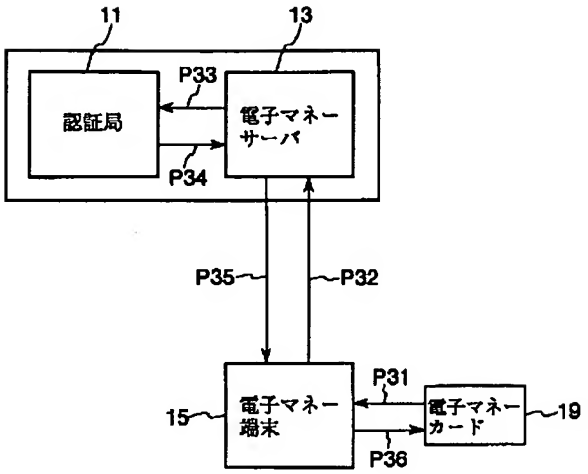
【図１３】



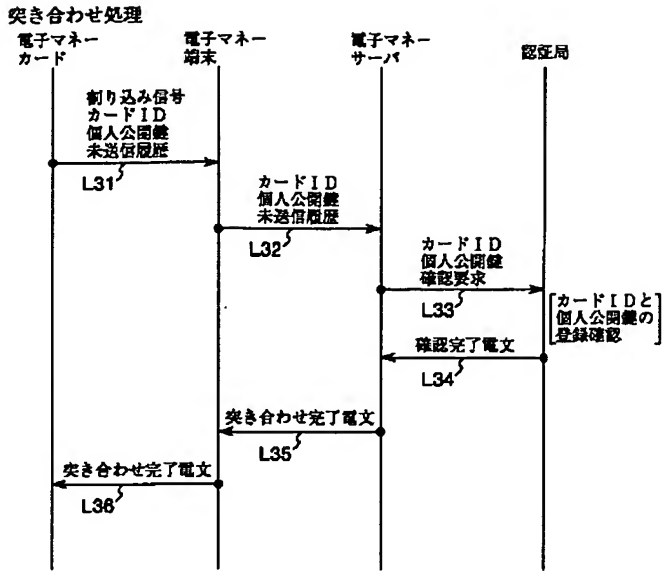
【図９】



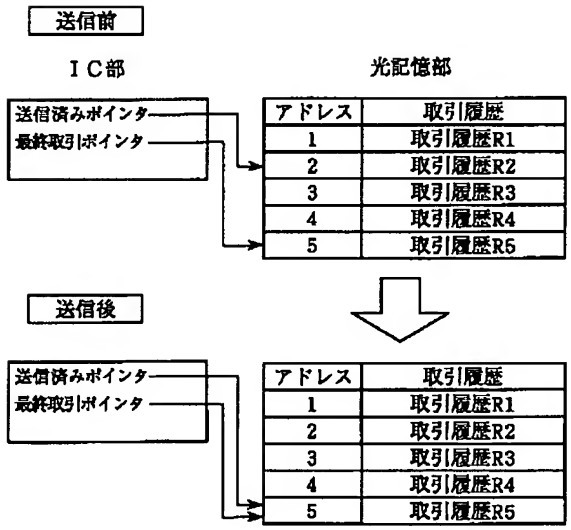
【図１４】



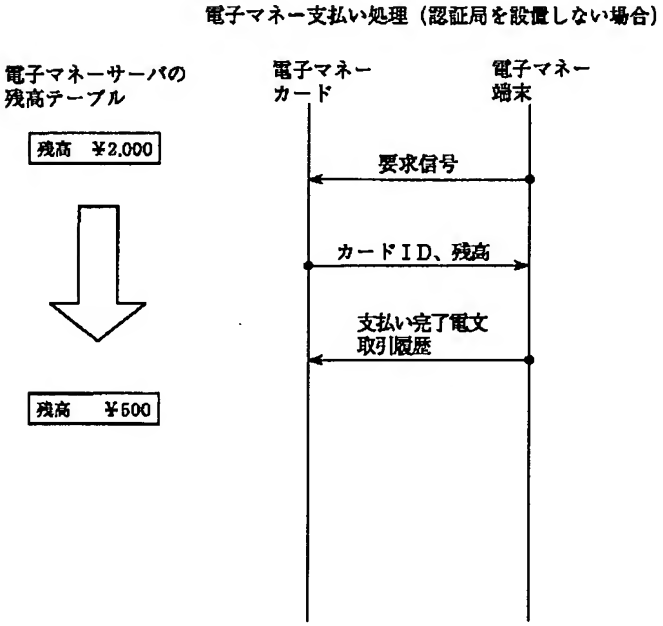
【図１５】



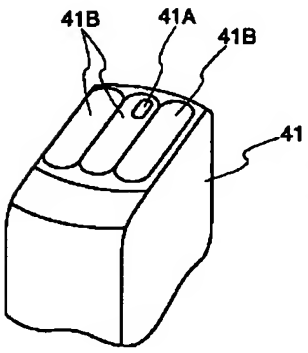
【図１６】



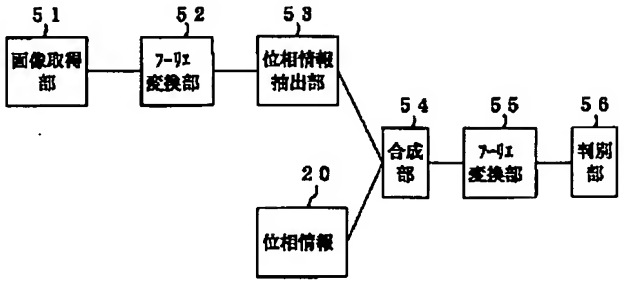
【図２３】



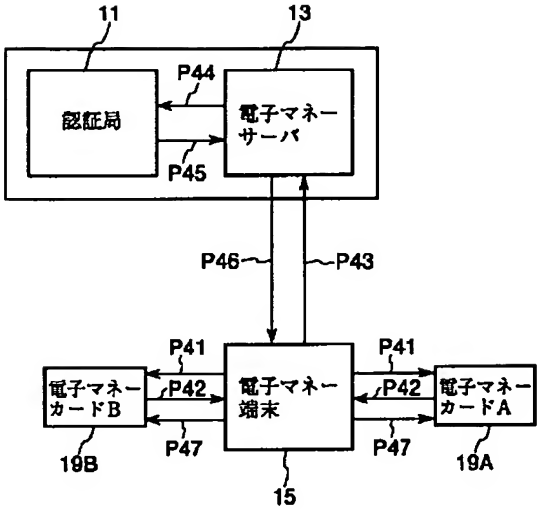
【図２７】



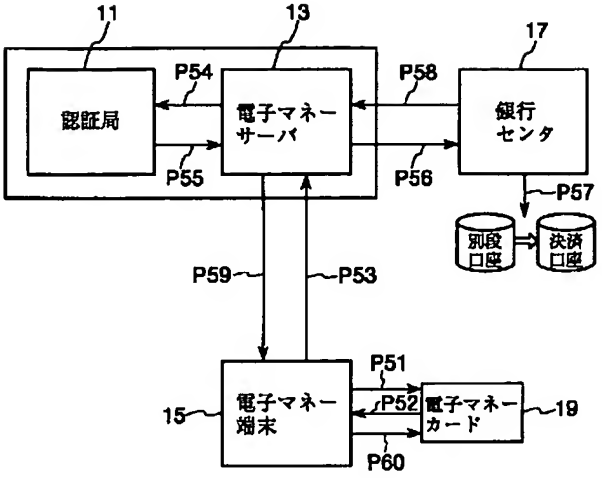
【図２８】



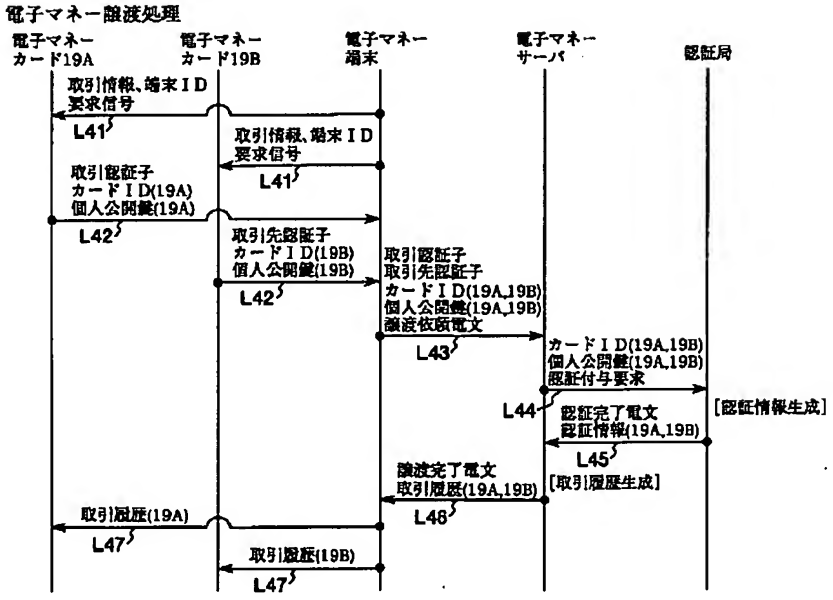
【図１７】



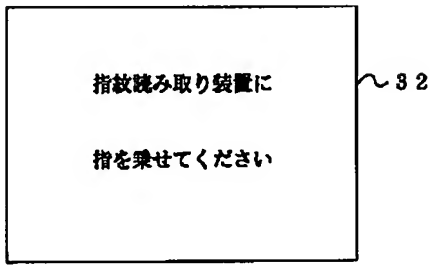
【図１９】



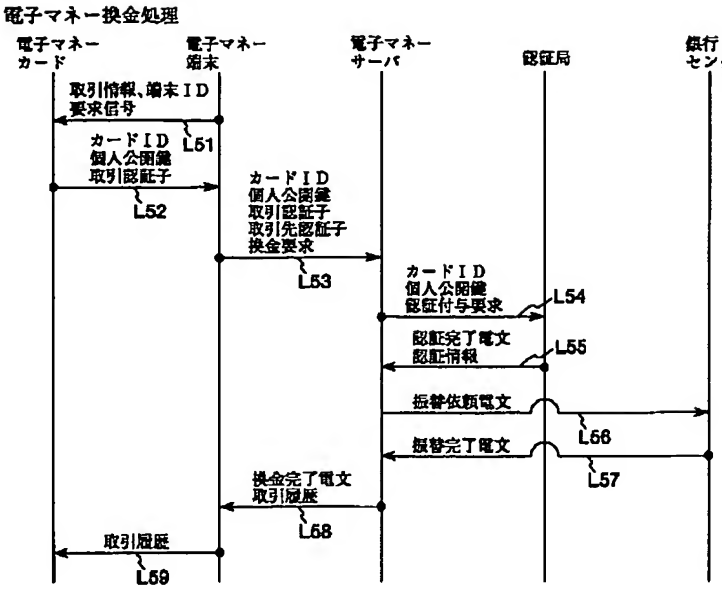
【図１８】



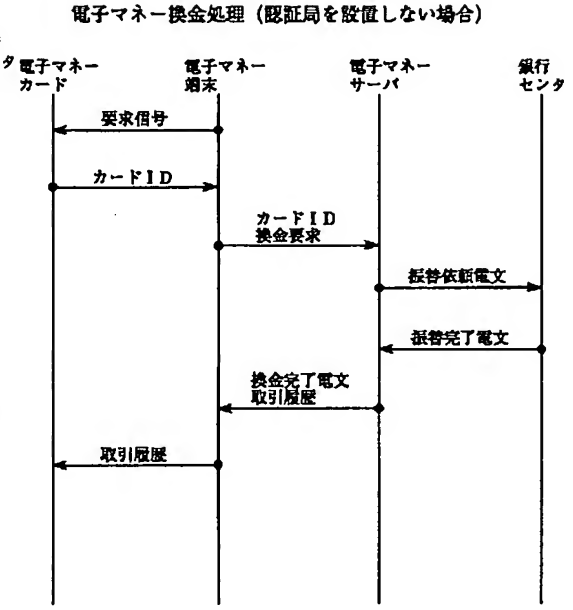
【図２９】



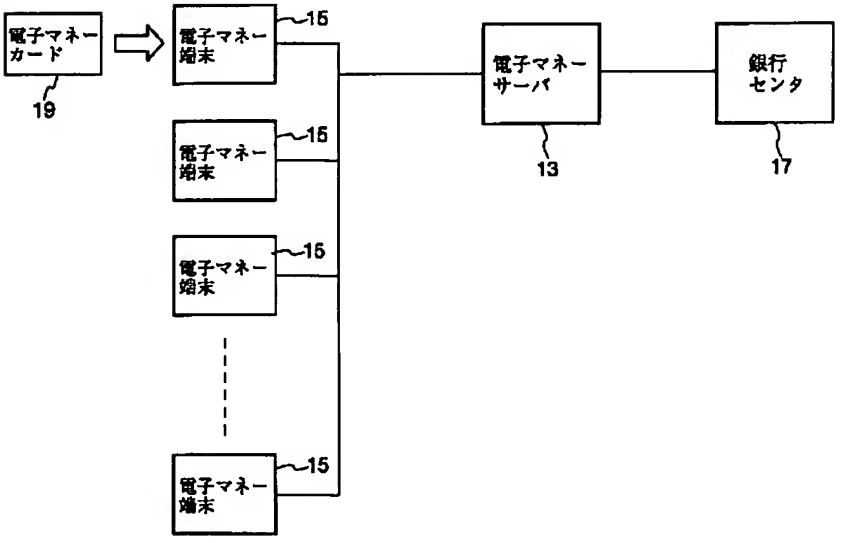
【図２０】


電子マネー換金処理
電子マネーカード
電子マネー端末
電子マネーサーバ
認証局
銀行センタ
取引情報、端末ＩＤ要求信号
L51
カードＩＤ 個人公開鍵 取引認証子
L52
カードＩＤ 個人公開鍵 取引認証子 取引先認証子 換金要求
L53
カードＩＤ 個人公開鍵 認証付与要求
L54
認証完了電文 認証情報
L55
振替依頼電文
L56
振替完了電文
L57
換金完了電文 取引履歴
L58
取引履歴
L59

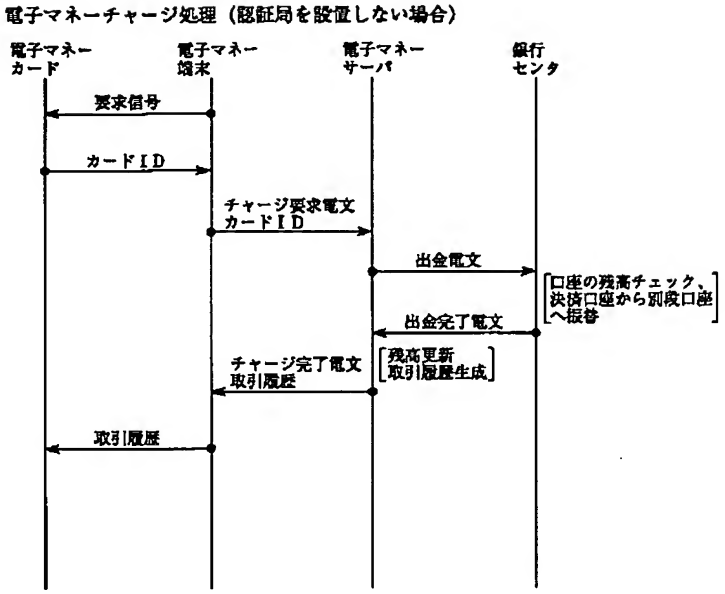
【図２６】


電子マネー換金処理（認証局を設置しない場合）
電子マネーカード
電子マネー端末
電子マネーサーバ
銀行センタ
要求信号
カードＩＤ
カードＩＤ 換金要求
振替依頼電文
振替完了電文
換金完了電文 取引履歴
取引履歴

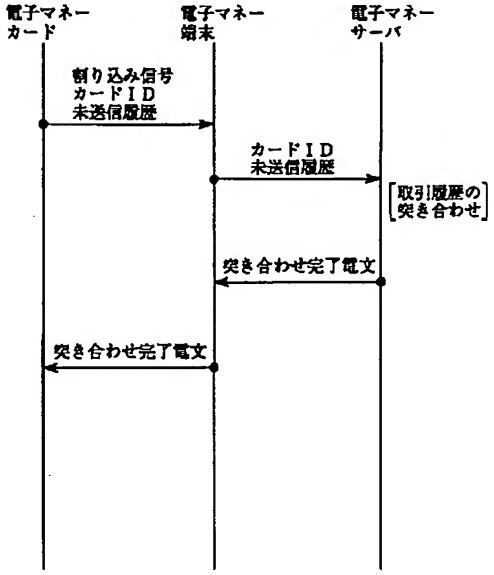
【図２１】


電子マネーカード
19
電子マネー端末
15
電子マネー端末
15
電子マネー端末
15
電子マネー端末
15
電子マネーサーバ
13
銀行センタ
17

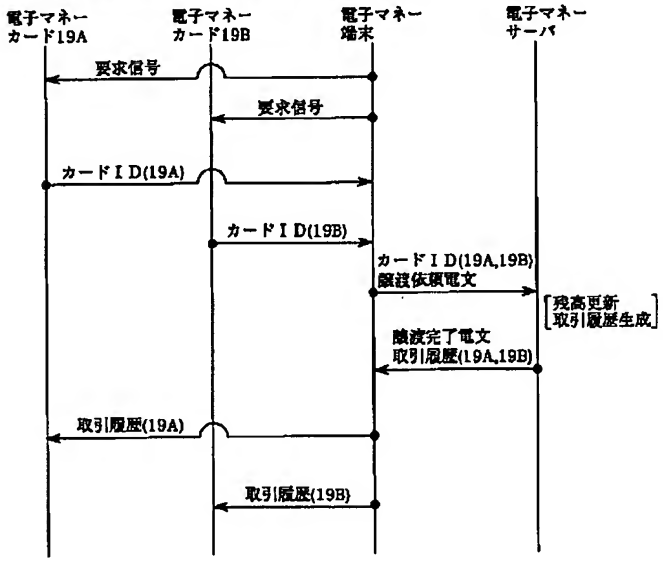
【図２２】



【図２４】



【図２５】



フロントページの続き

(51) Int.Cl.[6]	識別記号	FI	
Ｇ０７Ｆ　19/00		Ｇ０６Ｆ　15/30	３１０
7/08			３６０
		Ｇ０７Ｄ　9/00	４７６
		Ｇ０７Ｆ　7/08	Ａ

(72)発明者　佐藤　哲
東京都江東区豊洲三丁目３番３号　エヌ・
ティ・ティ・データ通信株式会社内